WASHINGTON STATE BAR ASSOCIATION

Advisory Opinion: **202402**

Year Issued: **2024**

RPCs: **1.6 and 1.0A, 1.1, 1.7, 1.8, 2.1, 5.1, 5.3, 5.4, 8.4(a)**

Subject: **Reporting Client Data to Legal Aid Funders**

ISSUE

What factors should a lawyer consider when deciding whether or how to report anonymized client data to a funder of legal aid services in a disaggregated format?

SHORT ANSWER

Under RPC 1.6, a lawyer shall not reveal information relating to representation of a client without client consent, other authority under the RPCs, or a court order. When considering a request for client data from a funder, the reporting lawyer should not rely solely on anonymization to report client data in a disaggregated format (defined below). The lawyer's reporting of information relating to representation of a client should instead be reasonably calculated to prevent reidentification of clients. The lawyer should consider relevant factors to assess the risk that data submitted to a funder could identify a client without authorization. Such factors may include, but are not limited to, the number of data fields requested, the degree of specificity requested, and the demographic characteristics of the clients served by the program.

When a reporting lawyer reasonably believes that data requested by a funder could lead to discovery of confidential client information, RPC 1.6 requires the reporting lawyer to act competently to safeguard that information. The reporting lawyer should provide the requested data only consistent with a funding agreement between the funder and the reporting lawyer, or funded legal aid organization, that contains provisions reasonably likely to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.

A lawyer who is advising a funding organization should be mindful of RPC 8.4(a).[n.1] The funding agreement between the funder and the legal aid organization must prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client. The reporting lawyer may not share client data that the lawyer reasonably believes will reveal confidential information solely to obtain or maintain a funding agreement.

TERMINOLOGY

"Aggregated data" refers to data that is combined across clients. In other words, data is aggregated when it is reported as a percentage (or total number) of client characteristics that fall into a particular category (such as geographic area, age, ethnic group, or gender identification).

"Anonymized data" refers to a client data set that omits, redacts, or otherwise suppresses explicitly identifying client data such as name, birthdate, or social security number while leaving other client data intact which are not generally regarded as identifying, such as age range, partial ZIP code, or gender. Due to the potential for even an anonymized data set to be combined with public or other available data to reidentify a client, as explained below, anonymization may not be sufficient by itself to protect client confidentiality.

"Disaggregated data" refers to data that is provided on a client-by-client or individualized basis – for example, in a row in a spreadsheet where each column tracks a unique data field for the same client. The facts considered in this advisory opinion do not involve requests for direct identification of the clients served. Therefore, all references in this opinion to disaggregated data assume the client data requested have been anonymized in some manner.

"Funder" refers to a source of funding for legal aid, which might be a government entity, a non-profit organization, or any other donor of funds earmarked for legal services. A funder is a third-party payer under RPC 1.8(f).

The phrase "information relating to representation of a client" for purposes of data transmission and storage is defined at Comment [19] to RPC 1.6; Comment [17] to RPC 1.0A.

The term "legal aid organization" refers broadly to a "legal service office," which was defined in WSBA Advisory Op. 183 (1990, amended 2009) as lawyers who provide legal services at reduced or no cost to indigent clients, and to other common uses in Washington such as a "qualified legal services provider" that provides not-for-profit legal services primarily for low-income clients. See Washington Admission and Practice Rule 1(e)(8).

The term "reasonable belief" and factors pertaining to reasonability are interpreted in RPC 1.0A (h), (i), (j) and RPC 1.6 Comments [18] and [19].

"Reidentification" refers to a process of identifying the client subjects of anonymized disaggregated data sets by combining and analyzing anonymized client data sets and publicly or otherwise available data sets.

The term "reporting lawyer" refers to a lawyer who provides anonymized client information to a funder, including lawyers in a supervisory role in a legal services organization, lawyers involved in direct representation at a legal services organization, and lawyers in private practice who contract with funders of legal aid services.

FACTS

Eight Washington legal services organizations ("Group") ask whether they are

permitted under RPC 1.6 to comply with a request for an increased volume of disaggregated client data from a funder. All of the Group members provide nonprofit civil legal aid to indigent clients, and their funders are generally government entities, including counties, municipalities, the Office of Civil Legal Aid and the Legal Services Corporation, or nonprofit foundations, such as the Legal Foundation of Washington.

In past years, Group members typically reported between ten and fifteen substantive datapoints per client. Characteristic examples of these datapoints have included: Year of Service; Legal Problem; Date Case Closed; Level of Service Provided; County of Residence; County of Dispute; Language; Race and Ethnicity; Gender; and Citizenship Status. The Group members believe that RPC 1.6 permits them to provide aggregated data about their clients, such as the percentage of clients who identify as members of a particular racial or ethnic group. They also acknowledge that some funders are subject to legislatively assigned functions, which may include specific data collection for specific programs or studies. To ensure quality control, effective and efficient delivery of legal representation, and accountability of contractors to applicable standards of professional service, some funders have historically required Group members to report anonymized client data on a disaggregated basis in addition to or in lieu of aggregated reporting.

This advisory opinion was requested after a funder asked the Group members for a significantly increased amount of client data, including nearly thirty datapoints, many involving deeply personal client information. Some of the new requests are similar to the normally requested information, like the types and timing of services provided to clients. Some, like residential data, are similar but more specific, including ZIP code and household size. Some are more personal, such as the client's sexual orientation or the client's gender identify or expression. Some relate to medical conditions, such as whether a client has a disabling medical condition and, if so, what type of disability.

The Group members expressed a concern that disclosing such a large amount of very specific anonymized data could possibly lead to re-identification of a particular client and, as such, violate RPC 1.6.

ANALYSIS

I. Duty of Confidentiality

RPC 1.6(a) prohibits a lawyer from disclosing confidential client information except under specified circumstances. Following substantial amendments to the RPCs in 2006, “confidential information” includes all information relating to the representation of the client, regardless of the source of that information, whether that information is publicly available, or whether that information constitutes a “confidence” or “secret.” See RPC 1.6, Comment [3] and [21].

When a lawyer shares anonymized data, the lawyer must take care in how that information is reported. Comment [4] precludes a lawyer from sharing information that "could reasonably lead to the discovery of [confidential] information by a third person." See RPC 1.6 and Comment [4]. The duty of confidentiality further includes a duty to safeguard confidential information from inadvertent disclosure or unauthorized access to that information. See RPC 1.6(c) and Comment [18].

Moreover, "[w]hen retaining or directing a nonlawyer outside the firm, a lawyer should communicate directions appropriate under the circumstances to give reasonable assurance that the nonlawyer's conduct is compatible with the professional obligations of the lawyer." See RPC 5.3 and Comment [3]. This responsibility applies even if the outside non-legal services are provided by a lawyer. Id. The extent of this obligation will "depend upon the circumstances," such as the experience and reputation of the outside non-service provider. Id.

In 1990 and 2009, we considered whether a legal aid organization may disclose information relating to the representation of a client to a funder. See WSBA Advisory Op. 1990-183 (amended 2009); and see RPC 1.6, Comment [21] ("The phrase "information relating to the representation" should be interpreted broadly . . . .") In WSBA Advisory Op. 1990-183, we interpreted RPC 1.6 to require lawyers to obtain informed consent from clients prior to disclosure of "information to third-parties that would disclose or lead to disclosure of information relating to the representation of a client . . . . " Id. at 1. See also WSBA Advisory Op. 1999-195 (considering disclosure of confidential client information in detailed billing statements to persons other than the client); and see ABA Formal Op. 95-393 (disclosure of client files to non-lawyer supervisors).

The guidance in our prior amended opinion remains generally accurate, as the opinion was amended subsequent to the 2006 amendments to the Washington RPCs. The Washington Supreme Court, however, has subsequently clarified the duty of care lawyers owe regarding confidential client information, especially in the context of evolving technologies. Updated guidance about proper data reporting to funders under RPC 1.6 thus is important for the practicing bar. This advisory opinion is intended to further guide lawyers who work for or advise both legal aid organizations and funders. See, e.g.s, RPC 1.1 comment [8]; RPC 1.6(c) and comments [18] and [19]; RPC 5.3 comment [3]; and see *State of Washington v. Johnson & Johnson, et al.*, Washington State Court of Appeals, Div. I, No. 84140-8-I [*appeal to Washington State Supreme Court pending*].

New technologies and practices for digital data storage and transmission are adopted rapidly in the legal profession.[n.2] In addition, the databases maintained by legal aid organizations and their funders --- and the relationships between them --- are enveloped by a diverse, shifting, and often opaque tangle of contracts, donors, private vendors, local, state, and federal disclosure rules, complex departmental structures, litigation, audits, news reporting, and external oversight, including oversight by voters and their elected representatives. Numerous local, state and federal regulations rely heavily on anonymization of data as the key to balancing the social utility of open access to data with privacy protections for sensitive data.[n.3]

Nevertheless, there is growing consensus that anonymized data are less protective of privacy than commonly assumed, because anonymized data can be combined with publicly or

otherwise available databases to "reidentify" anonymized individuals for a range of benign and less benign purposes, including marketing, digital harassment, criminal investigation, or to alleviate boredom. Lawyers must therefore avoid the assumption that the process of anonymizing data is by itself sufficient under RPC 1.6, particularly for long-term protection of client confidentiality.

When deciding how to respond to a client data request, a lawyer should thoroughly and thoughtfully evaluate the potential pitfalls of reporting client data in a disaggregated format, even when the data are otherwise anonymized. In this regard, it is important to acknowledge two principles from computer science and privacy research.

First, certain combinations of anonymized and commonly recorded data are often unique to a single person. For example, studies of U.S. census data have reported that a majority of the population is uniquely identified by the following combination: ZIP code, sex, and date of birth (including year).[n.4] Even these widely known empirical findings are somewhat dated, and the data science field has continued to develop new reidentification threats to client confidentiality. Lawyers who disclose client ZIP code, sex, and date of birth would presumptively violate RPC 1.6.

Second, it is possible to combine anonymized data with a publicly available database to discover unique patterns useful for reidentification of some of the subjects referenced in the anonymized data.[n.5] In general, as data are accreted with other data in larger and larger amounts over time, a corresponding risk of reidentification also increases. Such risk increases if a funder maintains such data without time limit or restrictions or from multiple, overlapping reporting sources. When a funder maintains such data, the reporting lawyer should consider how the client data being reported might be combined with other data because, once released, the reporting lawyer has little if any control over what the funder does with data in their possession.

In deciding what format to use in reporting information relating to the representation of a client, lawyers should consider engaging in dialogue with the funder about the nature and context of how the funder will protect the client data during transmission and storage. Data disclosure that poses a reasonable risk of reidentification of a client to a third party, discloses personal information about the client, or reveals the nature of legal representation of a client constitutes disclosure of confidential information under RPC 1.6. There is no exception that permits a lawyer to disclose confidential client information to a third party who is paying for the representation of the client. See RPC 1.8(f)(3).

Moreover, a lawyer should not routinely seek consent from a client to disclose disaggregated data to funders in a representation agreement as a condition of providing legal aid services. To obtain informed consent from the client to disclose confidential information, a lawyer must first present the risks and benefits of disclosure and advise the client about disclosure candidly and with independent, unconflicted judgment. See RPC 1.0A(e), 2.1, 1.7, and 5.4(c); and see RPC 1.6 Comment [26] "The decision to waive confidentiality should only be made by a fully informed client after consultation with the client’s lawyer or by a court of competent jurisdiction." It is difficult to obtain informed consent to this type of disclosure before a representation is underway, particularly in the case of vulnerable clients who face, for example, risks to personal safety, immigration consequences (for undocumented persons), or

potential liability in another jurisdiction from pursuing reproductive health care.

The effectiveness of such a consent ought generally to be determined by the extent to which a prospective client reasonably understands the material risks that the consent entails. The more comprehensive the explanation of the types of risks that might arise and the actual and reasonably foreseeable adverse consequences of the disclosures, the greater the likelihood that the prospective client will have the requisite understanding. Thus, if a prospective client consents to a particular type of data disclosure with which she is already familiar, then the consent ordinarily will be effective with regard to that type of disclosure. If the consent is general and open-ended, then the consent ordinarily will be ineffective, because it is not reasonably likely that the prospective client will have understood the material risks involved. See RPC 1.7 Comment [22]. In addition, the lawyer should explain when a disclosure benefits the legal aid organization to facilitate continuity of funding, rather than directly benefiting the individual client.

For example, a legal aid program might represent clients who are in government custody or otherwise subject to government authority. Some of these clients' demographic information may already be in the possession of a government funder as a result of the custody or other relationship. If the prospective client receives a thorough explanation of (i) the actual and reasonably foreseeable adverse consequences of disclosing (a) client information already in the possession of the funder and (b) additional information, if any, requested by the funder together with (2) an acknowledgement that the benefits of disclosure accrue to the legal aid organization, then the prospective client may have the requisite understanding to provide informed consent to disclosure of anonymized demographic information.

In reporting client representation data to funders, therefore, a lawyer must report those data in a manner that ensures the lawyer is neither disclosing confidential information of individual clients nor disclosing information that reasonably could lead to the discovery of confidential information. See RPC 1.6(a) and RPC 1.6(c). The lawyer must also act reasonably to ensure that the conduct of subordinate lawyers and staff and other non-lawyer assistants comports with the lawyer's duties. See RPC 5.1 and 5.3.

II. Ethical Considerations in Reporting Anonymized Data

Whether a reporting lawyer would be considered to have acted reasonably in providing anonymized data to a funder will necessarily depend on the circumstances. In general, a lawyer should consider at least three factors relating to whether anonymized client data may be disclosed to a funder in a disaggregated format. The reporting lawyer should also consider information gained through dialogue with the funder about the reporting format and security of anonymized client data.

A. Presentation of Anonymized Data in a Disaggregated Format

The likelihood that clients could be reidentified from anonymized data presented in a disaggregated format depends on a variety of factors, including the following:

The number of fields reported. The larger the number of disaggregated client data fields that are reported to a funder, the greater the risk that the data may be combined with publicly or otherwise available data to reidentify clients.

Whether disaggregated data is reported in a specific or generalized format. Some client data fields may be reported with a greater or lesser degree of specificity. For example, if a funder requests the clients' dates of birth, that information – when combined with other information – could potentially lead to reidentification. Other methods of providing age-related information, in order of increasing protection of client privacy, include: reporting the year of birth without month or day, reporting the client's age, or reporting an age bracket (such as younger than 18 years, 18 to 64 years, 65 years or older). Similarly, there are ways to generalize geographic information, such as by reporting only the initial two or three digits of the client's ZIP code or reporting the client's county of residence.

The demographic characteristics of the clients served by the program. The reporting lawyer should consider the foregoing factors in the context of the demographic characteristics of the program subject to the reporting requirements. For example, if the program serves a demographic population that is relatively narrow when compared to the broader service population, the qualifying characteristics for inclusion in the program may present an elevated risk. For example, if a program serves only transgender youth or only undocumented immigrants, those sensitive qualifying characteristics will automatically be associated with other client data reported in a disaggregated format and may facilitate reidentification.

When providing client data for clients who are members of much smaller demographic populations within the overall population of clients served, then the reporting lawyer should consider further limiting the number of fields (if any) that are reported in a disaggregated format. On the other hand, a lawyer reporting for a program that serves a large, diverse population might reasonably provide more data fields in a disaggregated format. In either case, the reporting lawyer may also choose to use an aggregated format to provide whatever demographic information is not submitted in a disaggregated format, resulting in a hybrid report that contains disaggregated data for some data fields and aggregated data for others.

A lawyer reporting for a legal aid organization that receives funding for multiple programs may also conclude that application of the above factors (and any other factors considered relevant under the circumstances) requires a different reporting format for different programs, even if those programs receive financial support from the same funder.

B. Dialogue with the Funder

When a reporting lawyer has concerns about providing the disaggregated data sought by the funder, the reporting lawyer should engage in dialogue with the funder to gather information about data formats and data transmission and storage practices of the funder. It may also be helpful for the reporting lawyer to understand the funder's goals and requirements which are met by gathering demographic data clients served by the reporting lawyer.

A lawyer advising a funder should remain mindful of of RPC 8.4(a) and respect a reporting lawyer's obligation of confidentiality under RPC 1.6..[n.6] In many instances dialogue with the funder may inform substantive provisions of the agreement between the funder and the legal aid organization that employs the reporting lawyer, such as the format of the report – disaggregated data, aggregated data, or a hybrid format.

Comment [3] [Washington Revision] to RPC 5.3 may provide additional relevant guidance by analogy for evaluation of the terms of an agreement between the legal aid organization and the funder. When a lawyer shares client information with a retained or associated nonlawyer outside the lawyer's firm – for example, by using an Internet-based service to store client information – RPC 5.3 and Comment [3] require the lawyer to ensure that the nonlawyer's participation is compatible with the lawyer's professional obligations.

Ethics opinions from other jurisdictions that apply Comment [3] to externally stored client data generally require the lawyer to take "reasonable care" to protect client data before engaging the outside service, and they typically describe "reasonable care" as including investigation of the outside nonlawyer's data security measures.[n.7] While enumeration of the precise terms of agreements between legal aid firms and funders to protect client data exceeds the scope of an advisory opinion, the reporting lawyer should minimally include consideration of the following issues:

- How many and which representatives, vendors, or other entities associated with the funder might have access to client data reported in a disaggregated format?

- What precautions will the funder take to protect the disaggregated client data against access by unauthorized internal actors and external actors in a manner consistent with the reporting lawyer's obligations under RPC 1.6?

- Will the reporting lawyer or clients of reporting lawyers be notified promptly by the funder of any breaches that result in access to the reporting lawyer's disaggregated data?

- How long will the funder retain client data in a disaggregated format, and how will destruction of the data be confirmed?

- Are there explicit limits on the purposes for which data may be used and a means for confirming that the data has been destroyed after use?

Endnotes:

N.1 "It is professional misconduct for a lawyer to . . . violate or attempt to violate the Rules of Professional Conduct, knowingly assist or induce another to do so, or do so through the acts of another." RPC. 8.4(a).

N.2 Matt Reynolds, *How ChatGPT and other AI Platforms Could Dramatically Reshape the Legal Industry*, ABA Journal (06/01/2023) ("Experts have warned AI can insert bias and discrimination into the justice system, raise security concerns for law firms, and bad actors could use it to spread misinformation.") accessed on 07/05/2023 at

<https://www.americanbar.org/groups/journal/articles/2023/how-chatgpt-and-other-ai-platforms-could-dramatically-reshape-the-legal-industry/>.

N.3 See generally Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1730, 1743 (2010).

N.4 See Ohm at 1705, 1719 and FN 81. The studies discussed in this article calculated the percentage of the population uniquely identified by this combination of attributes to range from 61% to 87%.

N.5 Id. In the example discussed at page 1719 of this article, a government agency in Massachusetts, intending to support medical research, released anonymized records of state employees' hospital visits to any researcher who requested them. Although the agency anonymized the records by removing names, addresses, social security numbers, and other fields it considered to be explicit identifiers, a researcher demonstrated that by combining the anonymized records with publicly available voter rolls, the subjects of the records could be reidentified.

N.6 The duty of confidentiality aligns with statutorily imposed duties of confidentiality. Lawyers for legal aid funders may be subject to additional legislative duties, including confidentiality. In the child welfare context, compare the Washington State Office of Public Defense at RCW 13.50.010(13) ("The Washington state office of public defense shall maintain the confidentiality of all confidential information included in the records."); and the Washington State Office of Civil Legal Aid at RCW 13.50.(14) ("The Washington state office of civil legal aid shall maintain the confidentiality of all confidential information included in the records, and shall, as soon as possible, destroy any retained notes or records obtained under this section that are not necessary for its functions related to RCW 2.53.045"). See also RCW 2.53.030(7)(b) (requiring legal aid programs to have a system allowing for production of case-specific information with the exception of confidential information protected by the United States Constitution, the state Constitution, the attorney-client privilege, and applicable rules of attorney conduct.). See also GR 31.1(f), (l)(5) (recognizing right of review of records disclosure decisions and an exemption for personal identifying information, including individuals' home contact information, Social Security numbers, date of birth, driver's license numbers, and identification/security photographs from public access requests.). Regarding reidentification risk in the context of government records, see generally *State of Washington v. Johnson & Johnson, et al.*, Washington State Court of Appeals, Div. I, No. 84140-8-I [*appeal to Washington State Supreme Court pending*].

N.7 For example, New York Opinion 842 (Sept. 10, 2010) identifies several steps, including: investigating and periodically reconfirming the third party's security measures, ensuring that the third party has an enforceable obligation to protect confidentiality and security, and staying current with legal developments and technological advances relating to confidentiality.

***

than the Washington State Rules of Professional Conduct may apply to the inquiry. The Committee's answer does not include or opine about any other applicable law other than the meaning of the Rules of Professional Conduct.