NACDL ETHICS ADVISORY COMMITTEE
Formal Opinion 13-01 (December 2013)

Question Presented:

The NACDL Ethics Advisory Committee has been asked by a Federal Defender the following question:

> Whether the federal defender staff lawyers' obligations to preserve client confidences and other confidential, privileged materials pursuant to Model Rules of Professional Conduct, Rule 1.6 is violated when a third party, the Administrative Office of the United States Courts (AO), takes over and manages the technology systems of the federal defender office, including specifically federal defender e-mail, case management programs, and statistical systems, that contain confidential and privileged information.

Background on the Question Presented

The Office of the Federal Defender making this inquiry has a computer system that is managed by two in-house Information Technology (IT) staffers. That Office's IT systems, like those of most federal defender offices, were designed to be independent of the AO and other third parties. At present the AO has no access whatsoever to the computer programs of the federal defender office.

The AO is a third party vis-à-vis the federal defender program.[1] Although the AO administers all matters within the United States Courts, including federal defender

[1] The Administrative Office of the United States Courts offers this self-description:

> Created in 1939, the Administrative Office of the United States Courts (AO) serves the federal Judiciary in carrying out its constitutional mission to provide equal justice under law. The AO is the central support entity for the Judicial Branch. It provides a wide range of administrative, legal, financial, management, program, and information technology services to the federal courts. The AO provides support and staff counsel to the Judicial Conference of the United States and its committees, and implements and executes Judicial Conference policies, as well as applicable federal statutes and regulations. The AO facilitates communications within the Judiciary and with Congress, the Executive Branch, and the public on behalf of the Judiciary. The agency is a unique entity in government. Neither the Executive Branch nor the Legislative Branch has any one comparable organization that provides the broad range of services and functions that the Administrative Office does for the Judicial Branch. The agency's lawyers, public administrators, accountants, systems engineers, analysts, architects, statisticians, and other staff provide a long list of professional services to meet the needs of judges and the more than 32,000 Judiciary employees working in more than 800 locations nationwide.

offices, neither the directors of the federal defender programs nor the federal defender staff attorneys report to the AO or take orders from the AO. Conversely, the AO is not an agent, contractor or employee of the federal defenders and is not susceptible to control, direction or supervision from federal defender programs. The AO is a third party to the defender attorneys and their individual clients, whose primary commitment is to the judiciary.

Three of the computer programs being used nationally by the federal public defender programs[2] contain ethically confidential information. The first system, *defenderData*, is a client case management program that records information about individual cases, can store documents from individual cases, and has a section that functions as an electronic case log.[3] The second program, the federal defender's e-mail system, Lotus Notes, contains innumerable messages concerning clients and cases, including e-mails from clients to staff lawyers and support staff. The third program, DSMIS, compiles and analyzes statistical data, including information that can be broken down to individual cases, revealing confidential matters relating to the representation of specific defender clients.

The AO recently announced, as a cost-cutting measure, that it will soon take over the IT systems of the federal defender offices and merge them with other existing computer programs already administered by the AO.

---

http://www.uscourts.gov/FederalCourts/UnderstandingtheFederalCourts/AdministrativeOffice.aspx.

[2] "[T]here are 80 authorized federal defender organizations. They employ more than 3,300 lawyers, investigators, paralegals, and support personnel and serve 90 of the 94 federal judicial districts. There are two types of federal defender organizations: federal public defender organizations and community defender organizations." http://www.uscourts.gov/FederalCourts/AppointmentOfCounsel.aspx.

[3] All 80 federal defender organizations in districts across the country have begun using a new web-based system, *defenderData*, to manage their case information; schedule events, generate, edit, index and search case-related documents, and produce reports. *defenderData* has been adapted exclusively for federal defenders and replaces a more than 15-year-old decentralized legacy system. Everything about a case, from information about clients and charges to case disposition can be accessed by a federal defender using *defenderData*. The system is user-friendly, able to generate reports on cases received, closed or pending, as well as reports on any variation of case-related data, including case assignments by attorney, time spent per case or by offense or other variables monitored by the federal defender organization.

Court Insider: New Defender Case Management System Debuts (November 20, 2012). http://news.uscourts.gov/court-insider-new-defender-case-management-system-debuts.

The AO has offered to promise not to view client confidential information contained in the defender office's three programs. However, as managers/administrators of the merged systems, AO personnel will have access to confidential and privileged information contained in these three computer programs.

The federal defenders and the Defender Services Office have strongly opposed the AO taking over these defender systems, noting that the exposure of confidential and privileged information to AO personnel, third parties, will compromise the confidential and/or privileged nature of the information in question. The AO has apparently rejected this analysis and is scheduled to merge the defender offices' IT systems with its own programs in early January 2014.

Ethical Issues

Confidentiality

Rule 1.6(a), *Confidentiality of Information*, ABA Model Rules of Professional Conduct,[4] provides that "[a] lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent …."[5]

As explained in Comment [3] to Rule 1.6:

> The principle of client-lawyer confidentiality is given effect by related bodies of law: the attorney-client privilege, the work product doctrine and the rule of confidentiality established in professional ethics. The attorney-client privilege and work product doctrine apply in judicial and other proceedings in which a lawyer may be called as a witness or otherwise required to produce evidence concerning a client. The rule of client-lawyer confidentiality applies in situations other than those where evidence is sought from the lawyer through compulsion of law. The confidentiality rule, for example, applies not only to matters communicated in confidence by the client but also to all information relating to the representation, whatever its source. A lawyer may not disclose such information except as authorized or required by the Rules of Professional Conduct or other law.

The duty of confidentiality includes not only attorney-client privilege and work product, but all information related to representation. "This prohibition" against the disclosure of confidential information "also applies to disclosures by a lawyer that do not in themselves reveal protected information but could reasonably lead to the discovery of such information by a third person." Rule 1.6, Comment [4].

---

[4] American Bar Association's Model Rules of Professional Conduct (2013).

[5] The wording of Rule 1.6 may vary from state to state more so than other adopted model rules. Lawyers are cautioned to consult local ethics rules.

The ethical duty of confidentiality, unlike the evidentiary attorney-client privilege, has no exception for previously disclosed or otherwise available information.[6] A lawyer may be subject to discipline for revealing confidential information even if a court decides that the attorney client privilege was waived by an unauthorized disclosure to a third party.

Confidentiality Survives the Termination of the Attorney-Client Relationship

The duty of a lawyer to maintain client confidentiality remains even after the attorney-client relationship has concluded. Rule 1.6, Comment [20]; Rule 1.9(c)(2). Consequently, the federal defenders must protect the confidentiality of information pertaining to their former clients as well as their present clients.

Federal Defender Computer Systems Contain Confidential and Privileged Information

The *defenderData* system, scheduled to be merged with the AO computer systems, contains everything about an individual client's case including specific information about the client and all case-related documents. Such a system contains readily identifiable confidential and privileged information on each federal defender client.

Communications between clients and their lawyers are protected by the attorney-client privilege, which also extends to communications between clients and their counsel's support staff, such as investigators, paralegals, and legal secretaries. Work product is information collected or created for litigation and is exempted from disclosure by the work product privilege. *See generally Hickman v. Taylor*, 329 U.S. 495, 510-11 (1947); *United States v. Nobles*, 422 U.S. 225, 238 n. 11 (1975).

IBM Notes (formerly IBM Lotus® Notes) is e-mail software that "includes messaging, applications and social collaboration." http://www-03.ibm.com/software/products/en/ibmnotes/. The e-mails in this system used by the federal defenders contain communications between clients and their attorneys and support staff as well as between defenders and the support staff about the clients' cases. Communications of this nature would inherently contain confidential and privileged information.

Even the program that compiles and analyzes statistical data relating to the work of the federal defenders can be reduced to individual cases and clients, resulting in

---

[6] However, "[a] lawyer who has formerly represented a client in a matter or whose present or former firm has formerly represented a client in a matter shall not thereafter … use information relating to the representation to the disadvantage of the former client except … when the information has become generally known." Rule 1.9(c)(1). This exemption from confidentiality for public information of a former client is available only to the former client's lawyer and not to third parties, such as the AO.

information relating to "the representation" of individual clients, which is confidential under Rule 1.6 and privileged under the work product doctrine. See *NACDL Formal Ethics Opinion No. 03-01* (January 2003) (discussing when an attorney's timesheets would be confidential and privileged under the work product doctrine).

The federal defender computer programs scheduled to be merged with and controlled by the AO contain information that is undoubtedly confidential under the rules of ethics and privileged under the attorney-client privilege and the work product privilege.

The Client's Informed Consent

"A fundamental principle in the client-lawyer relationship is that, *in the absence of the client's informed consent*, the lawyer must not reveal information relating to the representation." Rule 1.6, Comment [2] (emphasis added).

Federal defender attorneys and their supervisors lack the authority to allow a third party access to a present or former client's confidential information *without the client's informed consent*. "'Informed consent' denotes the agreement by a person to a proposed course of conduct after the lawyer has communicated adequate information and explanation about the material risks of and reasonably available alternatives to the proposed course of conduct." Rule 1.0(e), Terminology.

Without each federal defender's client, whether a present or former client, providing informed consent, the federal defenders are ethically prohibited from allowing their IT programs, containing confidential information pertaining to past and present clients, to be merged with the computer systems of a third party, in this case, the AO.

An exception to the duty of confidentiality is that a lawyer may disclose confidential information when "the disclosure is impliedly authorized in order to carry out the representation." Rule 1.6(a). Impliedly authorized disclosures of confidential information generally are governed by the specific circumstances of the individual case. Rule 1.6, Comment [5]. The merging of the federal defender's computer programs with those of the AO, granting the AO access to confidential information, is not the type of disclosure that "is impliedly authorized to carry out the representation." Rule 1.6(a). As a result, informed consent is required from the client.

Attorney-Client Privilege and Work Product Privilege are Controlled by the Client

The attorney-client privilege belongs to the client, not the attorney. *Hunt v. Blackburn*, 128 U.S. 464, 470 (1888). The attorney cannot waive the attorney-client privilege except with the consent of the client. Similarly, the work product privilege cannot be waived by counsel without the client's consent.

Lawyer's Duty to Prevent Unauthorized Access to Confidential Information

Rule 1.6(c) states "[a] lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." "Paragraph (c) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties …." Rule 1.6, Comment [18].

As a result of this ethical obligation, a lawyer may not stand by and allow the confidentiality of information to be compromised by administrative measures that breach, undermine or waive that confidentiality.

A Public Defender Program Must Protect Confidential Information

Rule 1.8(f) on Conflict Of Interest: Current Clients: Specific Rules, has special application to public defender programs. That section explains that:

> A lawyer shall not accept compensation for representing a client from one other than the client unless:
>
> (1) the client gives informed consent;
>
> (2) there is no interference with the lawyer's independence of professional judgment or with the client-lawyer relationship; and
>
> (3) *information relating to representation of a client is protected as required by Rule 1.6*.

(Emphasis added.)

An attorney will be subject to discipline for participation in a defender program that does not protect the confidential information in the attorney's past and present cases. A public defender agency, such as the federal defender program, has an obligation to ensure that confidential and privileged information pertaining to each and every one of its indigent clients, whether past or present, is protected in accordance with ethical rule 1.6.

That ethical obligation to protect the confidentiality of information relating to the representation requires federal defenders to make reasonable efforts to prevent either unauthorized disclosure or access. "A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." Rule 1.6 (c). This provision "requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision." Rule 1.6, Comment [18].

"A lawyer may be ordered to reveal information relating to the representation of a client by a court or by another tribunal or governmental entity claiming authority pursuant to other law to compel the disclosure." Rule 1.6, Comment [15]. This would appear to be the situation created by the AO seeking the merger of the defenders'

computer systems with its own programs. "Absent informed consent of the client to do otherwise, the lawyer should assert on behalf of the client all nonfrivolous claims that the order is not authorized by other law or that the information sought is protected against disclosure by the attorney-client privilege or other applicable law." *Id*.

As a result, it is the opinion of the NACDL Ethics Advisory Committee that federal defenders are ethically compelled in this instance to raise all colorable claims against this merger in whatever forums are available, absent informed consent by all their clients, past and present, to do otherwise. *See People v. Belge*, 50 A.D.2d 1088, 376 N.Y.S.2d 771 (4th Dep't 1975) (New York public health law should not be construed to require lawyer to reveal confidential information); Rule 1.6, Comment [15]; RESTATEMENT (THIRD) OF THE LAW GOVERNING LAWYERS § 60 (2000) & Comment e (the lawyer has a duty to assert and protect confidentiality)

The Need to Ensure That Confidentiality is Maintained

Apparently the AO has not provided the federal defenders with anything more than a promise that the merger of the defender computer systems with those of the AO will not compromise confidentiality. The AO has not provided the federal defenders with any specific written policies and procedures prohibiting unauthorized access to and/or control over the defender's confidential data once the merger of systems is completed. Absent such information, the federal defenders cannot even evaluate the workability of the proposed merger as to the preservation of confidential and privileged information. Under such circumstances, therefore, federal defenders cannot be certain that "information relating to representation of a client is protected as required by Rule 1.6."[7]

According to the merger proposal, AO staffers will have both access to and control of the confidential information contained in the defender computer programs. This in itself violates ethical confidentiality and such disclosures could constitute waiver of both the attorney-client privilege and the work product privilege contained in the information.

Conclusion

It is unethical for the Federal Defenders to participate in a data merger program that does not adequately protect confidential information for past and present clients.

[7] If such a policy or procedure is ever adopted, we will revisit this opinion.