



FEDERAL DEFENDER

Middle District of Florida

Donna Lee Elm
Federal Defender

James T. Skuthan
First Assistant Defender

February 17, 2016

The Honorable Kathleen Cardone, Chair
Ad Hoc Committee to Review the Criminal Justice Act
Thurgood Marshall Federal Judiciary Bldg., Ste. 4-210
One Columbus Circle, NE
Washington, DC 20544

Re: Testimony of Donna Lee Elm
Federal Defender, Middle District of Florida

Your Honor and Committee Members:

I have been the Federal Defender for the Middle District of Florida for almost 8 years. For 6 years before that, I was an Assistant Federal Defender for the District of Arizona. Having served an additional 12 years in the state public defender system in Phoenix, I have more than a quarter century of indigent defense representation experience – most being in federal courts in two very different jurisdictions. More importantly for my testimony, the Director honored me with an appointment as Chair of the Defender Automation Working Group (DAWG, the defender IT advisory committee) after having served a term as a member. The Director also appointed me as the lone Federal Defender member of the Joint Electronic and Technology Working Group (JETWG, a collaborative effort of DOJ and the defense to resolve electronic evidence concerns). As a result for the past 6 years, I have been immersed in how IT is used in our practice of law.

I also have a background in legal ethics. For a number of years, I served as volunteer Bar Counsel in Arizona. For the 6 years leading up to becoming a Federal Defender, I had been appointed by the Arizona Supreme Court as a trial-level judge for attorney discipline matters. I have served on an ethics committee, and have taught and published in the field of legal ethics.

ORLANDO DIVISION
Seaside Plaza – Suite 300
201 South Orange Avenue
Orlando, Florida 32801
Telephone 407 648-6338
FAX 407 648-6095

TAMPA DIVISION
Park Tower – Suite 2700
400 North Tampa St
Tampa, Florida 33602
Telephone 813 228-2715
FAX 813 228-2562

JACKSONVILLE DIVISION
BB&T Tower – Suite 1240
200 West Forsyth Street
Jacksonville, Florida 32202
Telephone 904 232-3039
FAX 904 232-1937

FT. MYERS DIVISION
Kress Building – Suite 301
1514 Broadway Street
Ft. Myers, Florida 33901
Telephone 239 334-0397
FAX 239 334-4109

OCALA DIVISION
Suite 102
201 S.W. Second Street
Ocala, Florida 34471
Telephone 352 351-9157
FAX 352 351-9162

As a result, I have deep concerns about two aspects of Defender IT: maintaining confidentiality and reliability of our data; and managing a national defender IT program.

Management of Defender IT Pre-Reorganization

Until a couple years ago, Defender offices and Defender Services (DSO) at the Administrative Office of the U.S. Courts (AO) largely managed the national IT program for federal defender offices.¹ While specific individuals involved varied over time, Defender IT maintained a strong leadership presence shared between several persons in DSO and the National IT Operations And Development (NITOAD). NITOAD was part of the Defender office in the Western District of Texas; it managed the technology, national communications and IT applications, and sometimes assisted in local offices' IT personnel. NITOAD staff also helped Defenders select suitable IT staff and performed audits of individual Defender offices' IT systems. DAWG functioned truly as an advisory group to this robust structure. It was always clear that the Chief of NITOAD took direction and assignments from DSO's head of Defender IT, the two entities worked closely together to execute IT directives for Defender offices.

Because the NITOAD Chief was an employee of the Texas Western District Federal Defender, it was situated in the "umbrella of confidentiality" of Defenders. Consequently, it was able to run the national email system Defender offices use to communicate with and defend clients. When there were technical problems with an IT program or data from a Defender office, NITOAD personnel could assist without running afoul of confidentiality concerns.

After sequestration's demand for cost containment in 2013, the AO decided to consolidate the IT programs of the various court units. Defender Services was informed that its IT program would be removed from Defender Services and moved to the newly created case management arm of the AO (the Case Management Services Office, CMSO). DSO would lose its Defender IT management staff..²

We recognize that all court agencies and the Court itself consider much of their data private or sensitive. The Federal Defender's offices are, however, the *only* branch of the U.S. Courts that in fact *represent clients*. Our data is full of client

¹ E-discovery and litigation support software was managed by the National Litigation Support Office.

² They would be replaced by a single IT Liaison to coordinate matters between DSO, CMSO, DAWG, and NITOAD.

confidential information and work product. We are, in that respect, materially different from other Court entities facing consolidation.

The Confidentiality Conflict

One of the problems that the Federal Defender program has had to deal with when it remains ensconced within the AO is educating and persuading other parts of the AO about the implications of this critical difference.

This matter was of considerable concern to Defenders. I was a member of DAWG when this occurred in the summer of 2013, and the DAWG Chair promptly authored a letter to the AO explaining that client confidentiality would be jeopardized, and protested this decision. The letter had no practical impact, and the plan to wholly remove our IT oversight was moving ahead unabated.

Discussion within DAWG was that perhaps the AO did not realize how seriously this would breach confidentiality. Relying on my background, I gathered ethics opinions from throughout the country regarding loss of privilege when client confidential information is exposed to third parties, and prepared a memorandum outlining the issues citing to ethics opinions.³ Mid-fall of 2013, the DAWG Chair sent a follow-up letter including information from the memorandum of ethics law, again explaining that we could not allow the AO (as a third party) to control Defender IT. Nevertheless, the letter again had no practical impact, and there were no changes in the plan to remove our IT communicated to DAWG or DSO.

³ The law, in short, holds that client confidentiality is waived when the lawyer allows a third party mere “access to” the confidential information – even when the third party has not in fact accessed it yet or agrees not to. A lawyer fails his ethical duties to the client by simply “exposing” confidences to an outside party. The seminal opinion was the Kansas Bar Association Ethics Opinion E-406 (1998), and a number of similar opinions from other jurisdictions and the ABA ensued.

Once waiver occurs, the defense is hard-pressed to avoid having thrown the doors open to discovery. Courts are familiar with this issue in litigation where the government seeks to introduce phone calls and emails between detained clients and counsel (where the corrections facility warns that those communiques may be recorded by the provider). If the AO became the third party provider of (with access to) email Defenders used to talk to clients, similar litigation would indeed be well-taken. Furthermore, if the case management system and case logs from defenderData (the case management program) were accessible to CMSO, then the government could legitimately subpoena our electronic case files because the Defense waived any claim to privilege by exposing them to a third party. This Committee should appreciate both the litigation havoc and the crucial Fifth and Sixth Amendment implications that this would create.

Patently, our ethical obligations to our clients required Defenders to ensure that third parties could not access our confidential information. With no acknowledgement of this concern from the AO, DAWG mobilized members to explore alternatives for managing our IT outside the AO. We looked into contracting with different email providers (individualized contracts for each of the 80-odd Defender offices).⁴ This presented a host of problems including no longer having a national email system, no longer having the cost-savings and management benefits of using a single email provider, and lack of skills and experience at the Defender office level to implement switching to and contracting with an email service provider. Interestingly, the cost of migrating to individualized office email alone surely exceeded the cost-savings anticipated by consolidating our IT with other IT management within CMSO.

Additionally, exploratory discussions began for Defender offices to directly contract with Justice Works to continue providing our critical defenderData application to offices. Again, there would be increased costs to this, and management would be difficult with Defender IT responsibility being stripped from DSO.

DAWG was of course not alone in protesting this merger. DSO similarly and actively sought to explain the administrative and cost problems to those making this decision. DSO noted that Defenders would be reluctant to use our national networking system (Defender Wide Area Network or D-WAN) to convey client information. This means that Defenders would no longer use their mobile devices to “remote in” to their office IT systems through the secure, firewalled internet channel maintained by NITOAD. This represented a significant step backwards in a program that was struggling to be on par with DOJ’s technological growth. DSO’s efforts similarly were to no avail.

In the meanwhile, the AO was hiring CMSO personnel to run (among other programs) the Defender IT program, and was drafting organizational plans to move Defender IT into CMSO.

⁴ The concern over the management of the FDO e-mail environment was so sensitive that the Defenders in the Ninth Circuit were investigating a Google mail deployment to replace Lotus Notes provided through the NITOAD Branch should it be managed by outside of DSO. This movement was gaining momentum with Defender offices in other circuits. The objection was to anyone outside of the DSO or its control having supervisory access to FDO systems, applications, and data. The reorganization ramifications would be devastating to the level of communication and collaboration between the Defender Community, DSO, the AO, and the rest of the Judiciary if Defenders implemented their own Google e-mail.

By late 2013, Defenders were gearing up to abandon the D-WAN as well as their email, case management, and any other IT systems that generated or held client information so as to comply with their ethical obligations of confidentiality. In December, the National Association of Criminal Defense Lawyers (NACDL) issued Formal Ethics Opinion 13-01 in support of the Defenders' concerns that client confidentiality would be compromised. Among its conclusions was the strongly worded advisement that:

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.

The Opinion stated that Federal Defenders were "ethically compelled" to raise all colorable claims against this removal. It concluded that it would be "unethical" for Federal Defenders to participate in this data merger. *See* NACDL Ethics Advisory Committee Formal Opinion 13-01 (December 2013), attached.

In the face of this Opinion, the AO remained non-responsive, but it did not go forward with consolidating the Federal Defender IT program into CMSO. By early January of 2014, the DAWG Chair asked to have the merger delayed 4 months while Defender offices implemented their own independent IT programs. Shortly thereafter, the AO agreed to move only administrative functions of Defender IT to CMSO, and that there would be no "access to" confidential information from outside NITOAD. Memoranda of Understanding (MOU's) confirming this were crafted and executed within a few months.

The critical take-away from this is: Federal Defender IT independence *necessarily* remains an *enormous concern* for our client representation to continue inviolate. Preservation of IT independence must be one of the highest priorities for the realization of the Fifth and Sixth Amendments in the Federal Defender system. The important recognition from this is: the AO was not appropriately responsive to the real needs of managing our law practices within the Courts' administration.

Management of Defender IT Post-Reorganization

While confidentiality has been preserved by these interventions, management of the Defender IT Program is more fractured than ever.

NITOAD continues to manage the substance of the national IT programs that Defender offices use. It remains within the “umbrella of confidentiality” as its staff is employed by the Federal Defender Office of Texas Western District. Direct supervision and direct administration of the NITOAD unit is handled by the Texas Western Federal Defender (presently Maureen Franco). The Chief consequently reports directly to his Defender, and is subject to her hiring, discipline, and firing. He is not technically an employee of CMSO.

However, per the AO’s organizational chart, the NITOAD Chief is directly supervised by CMSO. While said supervision is meant to extend only to the broad administration of IT systems (such as procurement, compliance, and inter-agency communications), it is difficult to draw the line between pure administration of an IT program and working directly with the program and its users. While CMSO cannot itself hire, discipline, or terminate the Chief of NITOAD, it would seem to have such authority by the organizational structure and is in fact directly very involved with supervising him. Though CMSO has tried to educate its staff as to the needs of Federal Defenders, it is not immersed in the our culture, and has not been in the business of a law practice. More importantly, its job as an arm of the AO is not to provide zealous representation. The essential mission differs.

Previously, direction for IT programming arose from DSO’s Defender IT staff and was often approved by DAWG. The 3 Defender IT staff though were replaced with an IT Liaison, a position lower in management and direction than its predecessor. There is consequently little leadership arising from within DSO regarding Defender IT development. While DSO does not supervise the NITOAD Chief, it has played an active role in decisions regarding personnel, and deciding changes in IT programming.

This leaves DAWG to step up and try to fill the void of deciding what direction Defender IT should go, and bridge the various differing interests of:

- Federal Defenders;
- NITOAD;
- the Defender in the Western District of Texas;
- DSO; and

➤ CMSO.

This was not DAWG's traditional role. To add to the confusion, Defenders have awakened to the key importance of preserving our IT program, and so the Defender Services Advisory Group (DSAG) now at times weighs in and intervenes in even minor IT changes as well.

➤ DSAG.

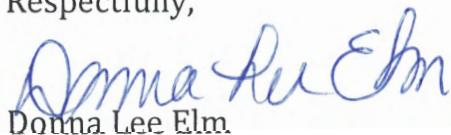
Nonetheless, DAWG was designed to function as an Advisory Group regarding the direction of the Defender IT program. The demands being placed on DAWG as a result, are beyond its intended scope.

This structure is hardly sustainable. It places an enormous strain on NITOAD staff being pulled in a myriad of directions. It places a different but substantial strain on the DAWG as well. Although efforts at collaboration have been made to date, this setup is ripe for serious conflict. DAWG constantly struggles to clarify what roles differing parties should play in this quagmire. It places both CMSO and DSO in untenable uncertainties about the extent of their authority and responsibility.

Criminal Justice Act Review

It is not my purpose to propose how to revise the Criminal Justice Act – a broad and terribly important function of this Committee – but as the DAWG Chair to highlight the management and representation needs of the Federal Defender IT Program. Regardless of Federal Defender independence in general, Defender IT independence must be preserved at all costs for both ethical and pragmatic management reasons.

Respectfully,



Donna Lee Elm

Federal Defender, Middle District of Florida
Chair, DAWG
Member, JETWG

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 programs² 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.