CLINICS, THE CLOUD, AND PROTECTING CLIENT DATA IN THE AGE OF REMOTE LAWYERING

ANDREW C. BUDZINSKI*

ABSTRACT

Technology has become central to law practice. Attorneys have an ethical obligation to understand how that technology works, how it can facilitate client representation—and the risks it poses to the confidentiality of clients' electronically-stored data. Law school clinics seem to fall behind the curve on this obligation. Some maintain outdated protocols, and some have no protocols at all, to manage and safeguard client data. This leaves client data less secure than it ought to be, risking harm to clients, ethical violations for attorneys, and missed opportunities to communicate the importance of ethical technology use to clinic students.

This Article offers a comprehensive overview of the potential ethical pitfalls relating to client data in law school clinics, and outlines the practical steps needed to avoid them. First, the Article describes the legal technology landscape, identifies what is at stake, and unpacks the many ways in which technology creates both opportunities and risks in the law school setting. Next, the Article surveys the ethical norms governing the use of technology with respect to client data under rules of professional conduct, the American Bar Association's leading ethics opinion on the topic, and state bar associations' various opinions. Finally, the Article lays out a series of questions and topics clinic law firms must answer to comply with ethical rules. For each, the Article proposes concrete steps that clinic personnel can take to reasonably protect client data in the unique context of universities, law schools, and clinical programs with student attorneys. This piece is meant to serve as both a wake-up call and blueprint to bring law school clinics into compliance with prevailing ethical norms around technology use and data privacy, to the extent they are not already in compliance.

* Assistant Professor of Law, University of the District of Columbia David A. Clarke School of Law, Co-Director of the General Practice Clinic. Many thanks to Sarah Boonin, Rachel Camp, Lindsay Harris, Marcy Karin, Mae Quinn, and my colleagues at the Mid-Atlantic Clinicians Writing Workshop and Clinical Law Review Writers' Workshop for their exceptionally helpful feedback. Additional thanks to my colleagues at UC College of the Law San Francisco, Suffolk University Law School, University of Arkansas at Little Rock William H. Bowen School of Law, and Pepperdine Caruso School of Law, who shared their clinical programs' technology use policies as I developed this project.

INTRODUCTION

Imagine you direct a law school clinic. You are teaching aspiring lawyers about the practice of law, direct representation, movement lawyering, racial justice, and the role of lawyers in safeguarding the dignity of the most underrepresented members of our society. You log in to an email inbox full of unread messages, when one catches your eye: an alert from your University's information technology ("IT") department. The University's cloud storage system through Microsoft OneDrive will be temporarily unavailable due to a data breach. To most, this is a minor inconvenience—a hassle to be sure, but also a now-familiar and expected risk of using cloud storage. But to a practicing lawyer and supervisor who uses OneDrive to store client work product, this is not merely a hassle. It is a potentially catastrophic moment of ethical dimensions.

As a supervising lawyer in the clinic, you are responsible for protecting client confidences and safeguarding client property—and for ensuring your third-party cloud storage provider takes reasonable steps to do the same.[1] Your students have uploaded all client work product to a folder in OneDrive, which you now cannot access. You learn that the data has been compromised—accessed and potentially duplicated by third parties who cannot be identified. You look back through the University's contract with Microsoft and realize that it does not contain any assurances about tracing who has accessed your client's data, what steps have been taken to safeguard it, or even limiting who will access the data at all.

Now, imagine the conversation with your client. You must inform them that their confidential information may be in the hands of someone else, and you do not know who, or where, or to what extent. Imagine the conversation with the administration; your University's general counsel; your jurisdiction's bar-ethics council. These are conversations that can be avoided, with understanding, planning, and forethought around technology use. And indeed, the rules of professional conduct require that understanding, planning, and forethought. This Article is meant to help clinical programs and clinical teachers do just that.

Cloud storage is one of many facets of modern law practice that brings with it important professional responsibility considerations.[2] Most client data is now electronic (either solely, or in addition to paper files), meaning the ethical lawyer must protect that data under

[1] *See infra* Part II.

[2] *See generally* MICHAEL R. DAIGLE, SHARON NELSON & ERIKA STILLABOWER, ETHICS AND THE CLOUD: A LAWYER'S DILEMMA (HOW PAINFUL CAN COLLIDING WITH A CLOUD BE?) (2018).

their duty of confidentiality,[3] to safeguard client property,[4] and to protect the attorney-client privilege and work-product doctrine.[5]

Moreover, to act "competently" under the rules of professional conduct, lawyers must "keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology."[6] In other words, it is incumbent on clinic faculty and supervising attorneys to understand how the technology they use works—not only how to use it, but how it technically generates and stores data. We must understand not only how technology enhances the practice of law, but also the risks that come with it. That means knowing where client data is stored when it goes to "the cloud," how third parties might access it, how it can be lost or misused, and what measures can be taken to reasonably protect it.[7] The American Bar Association (ABA) and many state bar associations have issued guidance applicable to handling and storing electronic client data,[8] and law firms have responded by adjusting their practice.[9]

Law school clinics, however, seem to fall behind the curve. While some clinics have identified and responded to the need for heightened client-data protections, others have maintained outdated protocols—or have no protocols at all—governing the management and safeguarding of electronic client data.[10] This gap matters for three key reasons. First and foremost, it puts a client's interests and dignity at risk by leaving their confidential data less secure than it ought to be. Second, it risks that clinic personnel are violating their ethical duties. And third, it fails to communicate to students the importance of safeguarding client data, and misses a critical opportunity to foster practice-readiness.[11] This matters even more as we continue to rely on the virtual communication and data-exchange tools used during virtual learning and the pandemic—though both students and law faculty employed those same tools well before 2020.

As ubiquitous as legal technology tools now are, the ethical implications of their use in the law school clinic setting have received relatively little attention. Some have raised the ethical issues at play in

---

[3] *See* MODEL RULES OF PRO. CONDUCT r. 1.6. (AM. BAR ASS'N, 2020).

[4] *See id.* at r. 1.15.

[5] *See id.* at r. 1.6 cmt. 3.

[6] *See id.* at r. 1.1 cmt. 8.

[7] *See infra* Section II.B.

[8] *See, e.g.*, DAIGLE ET AL., *supra* note 2, at 8–21; ABA Comm. on Ethics & Pro. Resp., Formal Op. 477 (2017) (hereinafter "ABA Formal Op. 477").

[9] Brittany Stringfellow Otey, *Millennials, Technology, and Professional Responsibility: Training a New Generation in Technological Professionalism*, 37 J. LEGAL PROF. 199, 215–24 (2013).

[10] *See infra* notes 53–65 and accompanying text. R

[11] *See* Stringfellow Otey, *supra* note 9, at 224–44. R

how law school clinics define their "law firm."[12] Others have explored the ethical considerations when non-clinical law school faculty engage in lawyering through the clinic law firm.[13] And still others have identified the ethical considerations involved when law professors practice law *outside* of law school clinics.[14] Other work has explored the specific role that technology plays in clinical pedagogy and student professional identity formation.[15] These are each essential pieces of the ethical puzzle.

This Article seeks to add to this important, but underdeveloped, body of scholarship. As I worked to shore up my own clinical program's data privacy policies, I was surprised to learn that there is relatively little organized guidance on how to do it. To that end, this Article offers a comprehensive overview of the potential ethical pitfalls relating to client data in law school clinics, and outlines the practical steps needed to avoid them. This piece is meant to serve as both a wake-up call and blueprint to bring law school clinics into compliance with prevailing ethical norms around technology use and data privacy, to the extent they are not already doing so.

In Part I, I begin by defining the technology landscape applicable to law practice and by identifying what is at stake. I unpack the many ways in which technology has become central to the practice of law, as well as the ways failure to engage that technology ethically can create challenges in the law school setting. I also posit that many clinics are lagging behind professional standards, and offer some possible explanations for why. Some clinicians and law school administrators may be more familiar with the ethical implications of technological change than others. Some may believe that their existing systems are more secure and compliant with ethical norms than they actually are. As clinics committed to upholding ethical obligations, protecting client interests, and training practice-ready lawyers, it is imperative that we model professionally responsible practice around technology.

Part II surveys the ethical norms governing the use of technology with respect to client data. It begins with a review of the duties related to competence, confidentiality, safeguarding client property, and su-

---

12 Nina W. Tarr, *Ethics, Internal Law School Clinics, and Training the Next Generation of Poverty Lawyers*, 35 WM. MITCHELL L. REV. 1011 (2009).

13 Laura L. Rovner, *The Unforeseen Ethical Ramifications of Classroom Faculty Participation in Law School Clinics*, 75 U. CIN. L. REV. 1113, 1179 (2007).

14 Gregory C. Sisk & Nicholas Halbur, *A Ticking Time Bomb? University Data Privacy Policies and Attorney-Client Confidentiality in Law School Settings*, 2010 UTAH L. REV. 1277 (2010).

15 *See, e.g.*, Margaret Martin Barry, Jon C. Dubin & Peter A. Joy, *Clinical Education for This Millennium: The Third Wave*, 7 CLIN. L. REV. 1 (2000); Sarah R. Boonin & Luz E. Herrera, *From Pandemic to Pedagogy: Teaching the Technology of Lawyering in Law Clinics*, 68 WASH. U. J. L. & POL'Y 109 (2022); Stringfellow Otey, *supra* note 9. R

pervising nonlawyer assistants. Then, it analyzes the reasonableness standards set out by the ABA and state bar associations regarding electronic client data. The part identifies the practices that afford client data reasonable protection under ethical rules.

In Part III, I lay out a series of questions clinic law firms must answer to comply with ethical rules. For each, I identify ways that clinic personnel can apply reasonableness factors in the unique context of universities, law schools, and clinical programs with student attorneys, and outline concrete strategies to do so. These areas and strategies include:

i. Ensuring that user agreements with case management software providers, cloud storage providers, and cloud-based email providers explicitly address the protection and ownership of client data;
ii. Creating agreements or understandings with relevant law school and/or university personnel to ensure that any client data on (a) university devices such as laptops, phones, and tablets, (b) university-funded cloud storage platforms, and (c) university web-based email servers is protected and continues to belong to the client alone, and not to the university;[16]
iii. Creating a policy and reasonable training for faculty, staff, and students[17] on appropriate protocols for accessing and transmitting client data, including through text message and email, access and storage of client data on personal devices, safeguarding search history,[18] not using personal cloud storage platforms to store client data, not accessing client data on public or unprotected Wi-Fi,[19] and not using personal email accounts to transmit client data;
iv. Creating internal agreements with university and/or law school IT staff that limit access to client data and, for those staff that work directly with client data and/or clinics, providing training on how they may and may not do so in compliance with the reasonableness standards; and
v. For public universities, creating an explicit policy on how client data will be identified, segregated, and protected from public disclosure under exceptions to freedom-of-information or "sun-

[16] *See* Sisk & Halbur, *supra* note 14. R

[17] *See* MODEL RULES OF PRO. CONDUCT r. 5.1 (AM. BAR ASS'N, 2020) (Responsibilities of a Partner or Supervisory Lawyer); *id.* at r. 5.2 (Responsibilities of a Subordinate Lawyer); *id.* at r. 5.3 (Responsibilities Regarding Nonlawyer Assistants).

[18] Anne Klinefelter, *When to Research Is to Reveal: The Growing Threat to Attorney and Client Confidentiality from Online Tracking*, 16 VA. J.L. & TECH. 1 (2011).

[19] *See* Mark Lanterman, *Is Emailing Confidential Information a Safe Practice for Attorneys?*, COLO. LAW., July 2018, at 19.

shine" laws.

The section culminates in a plan of action for law school clinics to implement to protect their client data, remain in compliance with rules of professional conduct, and ultimately recenter client dignity in these critical norms of law firm practice.

I. The Benefits and Perils of the Cloud

The role of technology in day-to-day lawyering has expanded dramatically over the last few decades.[20] Lawyers have come to employ a wide array of technology to handle essential components of law practice. For example, one survey of 190 legal professionals from law firms and in-house counsel positions found that respondents used technology tools for billing (79%), legal research (70%), e-signatures (69%), timekeeping (63%), cloud storage (62%), records management (59%), and matter management (53%).[21] Aside from practice management, technology has also become more widely used in litigation itself. For example, depositions can be conducted virtually through video conferencing applications.[22] And since the pandemic, many courthouses have retained at least some options for appearing in court virtually through video applications like Zoom and Webex.[23]

As the technologies of law practice have evolved, so have the forms of client confidences. Each technology creates new forms to generate, store, and transmit client information, creating what I will call client data. "Client data," as used in this piece, refers to any information protected by the duty of confidentiality[24] that is kept in an electronic format of any kind. This includes information on electronic case management systems, documents in electronic format (.doc, .pdf, etc.) and work product kept on cloud storage platforms or remote

[20] ABA Comm'n on Ethics 20/20, Introduction and Overview 3–7 (2012), https://www.americanbar.org/content/dam/aba/administrative/ethics_2020/20120508_ethics_20_20_final_hod_introdution_and_overview_report.pdf.

[21] Rachael Pikulski, Princess Onyiri & Linda Ouyang, *ANALYSIS: Lawyers' Top Legal Tech Tools—And Biggest Blind Spots*, Bloomberg Law (May 6, 2022), https://news.bloomberglaw.com/bloomberg-law-analysis/analysis-lawyers-top-legal-tech-tools-and-biggest-blind-spots.

[22] *See, e.g.*, Veritext Legal Sols., *Veritext Virtual*, https://www.veritext.com/services/veritext-virtual/ (last visited Jan. 27, 2023) (describing one company's specialized remote court reporting application).

[23] *See, e.g.*, Super. Ct. of D.C., Public Access for Remote Court Hearings (2023), https://www.dccourts.gov/sites/default/files/Public-Access-to-Remote-Court-Hearings.pdf.

[24] Of course, attorneys may also wish to protect other client information that does not fall within the scope of the confidentiality obligation. Many of the recommendations in this piece will also protect more than the rules require, and where they do not, attorneys can always take additional precautions.

servers, emails sent through web-based platforms, search histories on internet browsers, electronic communications with a client or others that include confidential information, and any other electronically stored client information that is owed a duty of confidentiality.

Without precautions and safe use, legal tech can create a risk that client data will be lost, inadvertently disclosed, or maliciously accessed, particularly when storing client data on cloud-based servers. Cloud computing involves "storing and accessing data and programs over the internet instead of your computer's hard drive."[25] Much technology used in the practice of law involves cloud storage, including web-based email, document storage, collaborative document-editing tools, and case management software. Without protections, client data can be subject to malicious data breach, inadvertently disclosed or destroyed beyond recovery, or, if stored outside the United States, go unprotected by a reasonable expectation of privacy akin to United States law.[26]

These risks are not hypothetical. As recently as July 2022, the FBI and other federal agencies warned of organized efforts to infiltrate cloud storage systems through phishing[27] communications, allowing third parties to ransom law firm data.[28] In 2010, the FBI warned law firms about attempts to maliciously access client data after two breaches at law firms in Hawaii.[29] These risks have manifested more broadly. Of law firms surveyed in 2021, 24.8% have experienced a security breach, and 29.2% reported their firm technology being infected with a virus, spyware, or malware.[30] While the majority of those breaches did not result in significant business disruption or loss,[31] in some cases firms needed to replace hardware or software, client files

[25] Eric Griffith, *What Is Cloud Computing?*, PCMAG (Feb. 15, 2022), https://www.pcmag.com/how-to/what-is-cloud-computing.

[26] *See* DAIGLE ET AL., *supra* note 2, at 1; *see also*, *e.g.*, Pa. Bar Assoc. Comm. on Legal Ethics & Pro. Resp., Op. 200, at 6, 9 (2011). R

[27] "Phishing" is "the practice of tricking Internet users (as through the use of deceptive email messages or websites) into revealing personal or confidential information which can then be used illicitly." *Phishing*, MERRIAM-WEBSTER.COM, https://www.merriam-webster.com/dictionary/phishing (last visited Jan. 27, 2023).

[28] *See* Peter Brown, *FBI Warns of New Cyber Threat to Clients*, N.Y.L.J. (July 11, 2022), https://www.law.com/newyorklawjournal/2022/07/11/fbi-warns-of-new-cyber-threat-to-clients/.

[29] Press Release, Honolulu FBI Press Office, U.S. Department of Justice, Federal Bureau of Investigation, Honolulu Law Firms Targeted in Financial Crime Wave (Feb. 22, 2010), https://www.abajournal.com/files/FBI_Press_Release.pdf.

[30] AM. BAR ASS'N LEGAL TECH. RES. CTR., 2021 AMERICAN BAR ASSOCIATION LEGAL TECHNOLOGY SURVEY REPORT: TECHNOLOGY BASICS & SECURITY 49, 51 (2021) (hereinafter "ABA 2021 TECHNOLOGY SURVEY"). Another 27.4% report they do not know if their data has been breached, *id.* at 49, and 32.1% did not know if their technology had been infected with a virus, spyware, or malware, *id.* at 51.

[31] *Id.* at 50, 52.

were destroyed or lost, and sensitive client data was accessed without authorization.[32]

In light of increased technology use and its risks, law firms have expanded efforts to ensure secure and ethical technology use. According to a 2021 ABA technology survey, a majority of all firms with two or more lawyers[33] have policies on email use (75%),[34] acceptable computer use (72.5%),[35] internet use (70.5%),[36] remote access to client data (72.5%),[37] disaster recovery and business continuity (59%),[38] and social media use (59.8%).[39] A substantial minority of such firms also have policies on incident response (45.9%)[40] and personal technology use or a "bring your own device" (BYOD) policy (40.6%).[41] Firms with ten or more lawyers are even more likely to have policies in those areas.[42] Generally, the larger the firm, the more likely it is that the

[32] *Id.*

[33] While the survey results include solo practitioners, the total percentages in the text accompanying notes 34–41 exclude them for two reasons. First, solo practitioners were significantly less likely to have technology security policies across the board, possibly because they feel a lesser need to formally prescribe their own behavior. Second, law school clinics are never solo practitioner firms, and always include at least two individuals (at least one supervisor and one student). Indeed, the statistics for firms with ten or more lawyers are likely even more relevant to clinical programs that combine all in-house clinics into one firm, and are therefore likely to have ten or more supervisors and students at any one time. For completeness, I include data from solo practitioners and firms with two to nine lawyers in each accompanying footnote. R

[34] *See* ABA 2021 TECHNOLOGY SURVEY, *supra* note 30, at 39 (27% of solo practitioners, 52.1% of firms with two to nine lawyers; 70% of firms with ten to 49 lawyers; 79.2% of firms with 50 to 99 lawyers; 80% of firms with 100 to 499 lawyers; 95.3% of firms with 500 or more lawyers). R

[35] *Id.* (21.3% of solo practitioners, 50.7% of firms with two to nine lawyers; 70% of firms with ten to 49 lawyers; 70.8% of firms with 50 to 99 lawyers; 75.6% of firms with 100 to 499 lawyers; 93% of firms with 500 or more lawyers).

[36] *Id.* (24.7% of solo practitioners, 42.5% of firms with two to nine lawyers; 64.3% of firms with ten to 49 lawyers; 79.2% of firms with 50 to 99 lawyers; 82.2% of firms with 100 to 499 lawyers; 93% of firms with 500 or more lawyers).

[37] *Id.* (18% of solo practitioners, 49.3% of firms with two to nine lawyers; 68.6% of firms with ten to 49 lawyers; 75% of firms with 50 to 99 lawyers; 77.8% of firms with 100 to 499 lawyers; 93% of firms with 500 or more lawyers).

[38] *Id.* (23.6% of solo practitioners; 38.4% of firms with two to nine lawyers; 51.4% of firms with ten to 49 lawyers; 62.5% of firms with 50 to 99 lawyers; 68.9% of firms with 100 to 499 lawyers; 79.1% of firms with 500 or more lawyers).

[39] *Id.* (21.3% of solo practitioners; 30.1% of firms with two to nine lawyers; 55.7% of firms with ten to 49 lawyers; 54.2% of firms with 50 to 99 lawyers; 73.3% of firms with 100 to 499 lawyers; 90.7% of firms with 500 or more lawyers).

[40] *Id.* (12.4% of solo practitioners; 20.5% of firms with two to nine lawyers; 35.7% of firms with ten to 49 lawyers; 54.2% of firms with 50 to 99 lawyers; 55.6% of firms with 100 to 499 lawyers; 79.1% of firms with 500 or more lawyers).

[41] *Id.* (11.2% of solo practitioners; 17.8% of firms with two to nine lawyers; 30% of firms with ten to 49 lawyers; 41.7% of firms with 50 to 99 lawyers; 53.3% of firms with 100 to 499 lawyers; 72.1% of firms with 500 or more lawyers).

[42] *See supra* notes 34–37. R

firm has a policy on each area of technology security and use.[43]

Similarly, firms with two or more lawyers[44] employ a wide range of security tools to protect client data and firm tech. These tools include: spam filters (81.5% of firms); firewall software (74.4%) or hardware (57.5%);[45] anti-spyware (72.4%); mandatory passwords (76.8%); virus scanning for email (70.9%), desktops/laptops (67.3%), and networks (70.9%); pop-up blockers (65.7%); encryption of files (57.1%), emails (47.6%), and hard disks (30.3%); two-factor authentication (50.8%); restrictions on file access (55.1%); intrusion prevention (37.8%) and detection (38.2%); remote device management and wiping (39.8%); web filtering (33.1%); and device recovery (27.2%).[46] As above, firms with ten or more employees were even more likely to use these security tools.[47]

Matching the broader legal field, law school clinics have also adopted legal technology as a central part of their practice. Many law school clinics use commercial case management systems to store information about clinic clients and to run conflicts checks.[48] The overwhelming majority of those use the no-cost platform offered by Clio.[49] Some clinics store client documents on cloud storage platforms like Box,[50] Microsoft OneDrive,[51] and Dropbox.[52] Clinics may use univer-

[43] *See* ABA 2021 TECHNOLOGY SURVEY, *supra* note 30, at 49. Slightly more firms with ten to 49 lawyers (55.7%) have a social media policy than firms with 50 to 99 lawyers (54.2%). *Id.* R

[44] As above, I exclude solo practitioners because, by definition, no clinic law firm has only one lawyer.

[45] "A firewall is software or hardware that can be configured to block data from certain locations, applications, or ports while still allowing relevant and necessary data to pass through. Firewalls are used to block unauthorized access to or from networks that have different levels of trust. They work by enforcing security policies and are used to prevent malicious actors from gaining access to private networks connected to the Internet. A firewall may be implemented through hardware, software or a combination of both." *Firewall*, TECHOPEDIA.COM, https://www.techopedia.com/definition/5355/firewall (Aug. 30, 2021). Hardware is "the physical elements that make up a computer or electronic system," *Hardware (H/W)*, TECHOPEDIA.COM, https://www.techopedia.com/definition/2210/hardware-hw, (Nov. 27, 2020), while software is "programs instructing a computer to do specific tasks" and "[e]verything that 'runs' on a computer, from an operating system, to a diagnostic tool, video game, or app," *Software*, TECHOPEDIA.COM, https://www.techopedia.com/definition/4356/software, (Mar. 31, 2020).

[46] *See* ABA 2021 TECHNOLOGY SURVEY, *supra* note 30, at 41. A far smaller percentage of firms also use employee monitoring (19.5%) and biometric login (10.5%). *Id.* R

[47] *Id.*

[48] ROBERT R. KUEHN, MARGARET REUTER & DAVID A. SANTACROCE, 2019–20 SURVEY OF APPLIED LEGAL EDUCATION, CTR. FOR THE STUDY OF APPLIED LEGAL EDUC. (CSALE) 36 (2020).

[49] *Id.* (finding clinics use Clio (69%), Time Matters (8%), Legal Server (8%), ClinicCases (2%), and Amicus (2%)); *see generally* CLIO, https://www.clio.com (last visited Jan. 27, 2023).

[50] BOX, https://www.box.com/home (last visited Jan. 27, 2023).

[51] MICROSOFT, *One Drive Personal Cloud Storage*, https://www.microsoft.com/en-us/

sity email accounts to send and receive client-related correspondence. Many clinic students and supervising attorneys use university or personal laptops or tablet devices to generate work product using applications like Microsoft Word or Google Docs. And many clinic students and supervising attorneys use personal smart phones or mobile devices for clinic-related calls, text messages, and email.

In the winter of 2021, Professors Sarah Boonin and Luz Herrera surveyed clinical faculty to ascertain the use and management of legal technology in clinics.[53] Responses showed that clinics overwhelmingly made use of the more standard options in legal technology. Ninety-five percent of respondents used "collaborative or team-based tools" like "OneDrive, Google Drive, and Microsoft Teams."[54] Ninety-one percent used some case management system, with 68% using Clio's cloud-based system.[55] Predictably, all respondents used email accounts and phones of some kind.[56]

However, clinics' data privacy protections were far less robust. Only 39% of respondents used remote access technology like virtual private networks[57] (VPNs) and virtual desktop infrastructures[58] (VDIs).[59] Only 39% used clinic-specific email accounts,[60] and 46% used email encryption to protect emails and attachments.[61] Forty-three percent of faculty respondents used personal cell phones for client work, while 19% used Google Voice and 13% used call forwarding.[62] Perhaps most troubling, while 84% of clinicians report providing some training on proper technology use, only 54% of clinics train stu-

microsoft-365/onedrive/online-cloud-storage (last visited Jan. 27, 2023).

52 DROBOX, https://www.dropbox.com (last visited Jan. 27, 2023).

53 *See* Boonin & Herrera, *supra* note 15, at 111 ("The survey received 121 responses from clinicians in 31 states and Puerto Rico."). R

54 *Id.* at 127.

55 *Id.*

56 *See id.* at 129–31.

57 A virtual private network "is a private network connection that is built over a public network infrastructure such as the internet. Security mechanisms, including encryption and hiding the user's IP address, allow authorized VPN users to access their corporate network remotely. VPNs are also useful for protecting personal information in public Wi-Fi settings . . . ." *Virtual Private Network (VPN)*, TECHOPEDIA.COM, https://www.techopedia.com/definition/4806/virtual-private-network-vpn (Aug. 30, 2021).

58 A virtual desktop infrastructure "is a shadow copy of the desktop including its [operating system], installed applications and documents, which are stored and executed entirely from the server hosting it. VDI provides users the ability to access their desktop remotely . . . ." *Virtual Desktop Infrastructure (VDI)*, TECHOPEDIA.COM, https://www.techopedia.com/definition/26809/virtual-desktop-infrastructure-vdi (Feb. 1, 2017).

59 *See* Boonin & Herrera, *supra* note 15, at 128. R

60 *Id.* at 129–30.

61 *Id.* at 130.

62 *Id.* at 131. The survey found that a higher percentage of students, as compared to faculty, used Google Voice. *Id.*

dents on data security, specifically.[63] Moreover, as the survey authors concluded, "[t]he majority of clinicians surveyed . . . do not appear to provide their students with written data security policies—and a substantial proportion of programs surveyed have no such policies at all."[64] It is unclear what respondents' "training" on data security entails.

The apparent shortfalls in clinic technology security have unique implications, in addition to those that apply to all legal professionals. University policies are not crafted with the same considerations as law firm policies—likely, they are crafted to protect the university and its students, not clinic clients. This raises a number of potential concerns. For example, when a law professor uses university cloud storage to keep client data, does the cloud storage company have a right to claim ownership over the data? Does the university? Is there a process through which the company will inform the university of data loss? Will the university inform the law school clinic? Where a law professor stores client data on a laptop provided by the university, does the university have an ownership interest in that data?

Similarly important questions arise around use of web-based email services, many of which operate through cloud-based servers. This means emails are also stored on remote servers maintained by the provider. If the university has not specifically contracted on it, those emails may be subject to the same questions raised above around cloud storage. Even if the university has contracted to create specific protections on email data, it can still raise ethical challenges. If students are not clearly instructed otherwise, they may send emails from or forward emails to their personal email, losing the protections university email can provide. Even general university email accounts may pose challenges where alumni can continue to access the account after graduating, meaning they can continue to access that data without the clinic law firm's oversight to ensure security. This is particularly problematic when a student automatically forwards their email to their personal account. University email accounts themselves are often accessible by non-clinic university employees, such as IT staff and general counsel. University emails are potentially discoverable.[65]

---

[63] *Id.* at 131 n.122.

[64] *Id.* at 132.

[65] Some, but not all, emails containing client data may be shielded by the attorney-client privilege and work-product doctrine. *See, e.g.*, Adam C. Losey, *Clicking Away Confidentiality: Workplace Waiver of Attorney-Client Privilege*, 60 FLA. L. REV. 1179, 1186–1201 (2008). However, university personnel charged with reviewing and responding to discovery requests must know how to segregate and shield emails protected by either; without a system in place, there is a serious risk such emails will be released without the responsible attorney having the opportunity to prevent it. For that reason, some universities have de-

And university email accounts at public law schools may be subject to a jurisdiction's freedom of information laws.[66]

It also matters which devices are used for clinic-related work. Storing client documents on a student's personal computer—such as interview notes, a draft direct examination, or track-changes to a draft contract—may open that client data up to unauthorized access. If a student were to work on a clinic client matter using public Wi-Fi in a café, any data transmitted on that unsecure wireless network could be accessed maliciously. Even if working from a more secure personal Wi-Fi connection at home, if a student's personal device becomes infected with a virus or spyware, or is otherwise accessed maliciously, third parties could obtain a client's data. And if the student comingles client data with personal data, they may open their personal data up to discovery or freedom of information requests (for example, by forwarding client-related emails to their personal email accounts).

These are just some of the issues that can arise in law school clinics. As these hypotheticals show, it is imperative that law school clinics structure their use of technology to meet the ethical and fiduciary standards owed to clinic clients. Despite that, some clinics' practices—perhaps many—do not comport with industry standards.

There are many possible explanations for these deficits, though it would be difficult to quantitatively determine which are primarily responsible. For one, prevailing models of clinical pedagogy grew in a context that did not include data privacy. The "second wave" renaissance of clinical legal education occurred in the 1960's,[67] well before technology revamped law practice.[68] As a result, the principal architects of prevailing clinic models designed clinic prototypes without considering data privacy—because that need did not exist yet. In many ways, the non-hierarchical "guided discovery learning" model of clinical education[69] itself cuts against top-down policies on how and

veloped specific protocols for responding to discovery requests that include university emails. *See, e.g.*, UNIVERSITY COUNSEL, STATE UNIV. OF N.Y., LEGAL PROCEEDING PREPARATION (E-DISCOVERY) PROCEDURES (2014), https://www.suny.edu/sunypp/documents.cfm?doc_id=752.

66 Serge Martinez, Univ. of N.M. Sch. of L., & Gabril Pacyniak, Univ. of N.M. Sch. of L., Developing an Open Records Act Strategy at a Public University Clinic, Presentation at the AALS Conference on Clinical Legal Education (Apr. 29, 2021); *see also infra* Section III.F.

67 *See* Barry et al., *supra* note 15, at 12. R

68 *See* Boonin & Herrera, *supra* note 15, at 112–13 & nn. 10–12. R

69 *See, e.g.*, DAVID F. CHAVKIN, CLINICAL LEGAL EDUCATION 7–15 (2002) (describing the "kitchen organizer" hypothetical to explain the pedagogical approach of guided discovery learning, in which the professor "ask[s] . . . a series of questions to help . . . identify the issues [the student] would have to confront," then "step[s] back to let [the student] begin the process and . . . observe[s] [the student's] work at particular intervals," and then finally "help[s] [the student] reflect on the steps . . . undertaken" in their work and "consequences

how not to use technology in practice. And, those clinical teachers who entered law practice before the technology boom may be less likely to incorporate technology into law practice, or less likely to identify the risks of its misuse.

The tenets of clinical pedagogy and client-centered poverty lawyering can also be in tension with data privacy norms. For example, in my early years of clinical teaching, I challenged students to explain why they would not communicate with their clients through their personal cell phones. I hoped to lead students to see the difference between boundary-setting and zealous advocacy, to identify their own biases around clients in poverty, and (if they chose) to test out what it would be like to give a client their mobile number to communicate by text message. As a matter of pedagogy, this seems to me an effective opportunity for student reflection (whatever their choice). As a matter of poverty lawyering, it may be a client-centered choice to create an easy, accessible avenue of communication between client and lawyer, like text message. As a matter of data privacy, though, it is risky to allow confidential client communications to live on students' personal smart phones without additional protections.

At a higher level, there may be a sense, conscious or unconscious, that data relating to pro bono clients does not require the same protection as highly resourced clients served by law firms. Some might operate on an unstated assumption that the consequences of a data breach would be less for the low-income client in a custody case than the wealthy corporate client that law firms often serve. Others might think it excusable to be more lax if the client has not inquired about how their data will be stored, perhaps also thinking it less likely that they will be held to account through ethics complaints or malpractice suits. Others might simply think the risk of a data breach is not as great when the legal matter involves low-income clients out of the public eye. These assumptions are, of course, antithetical to the very premises of poverty lawyering and based on a series of stereotypical assumptions—they degrade our clients, devalue their dignity, and risk real harm.

My students represent survivors of domestic violence in protection order cases. A savvy abusive partner could discover the holes in unsecure technology, or subpoena my University for our client's data. A University employee may not know the data is protected and release it. Or, a University employee may know the abusive partner and leak the data, which the clinic law firm has not prevented the employee from accessing. If any of this happened, it would be my respon-

[the student] experienced or were likely to experience from those choices").

sibility—it would not be an exceptional and unforeseeable fluke, but a direct consequence of my firm's failure to take reasonable steps to protect client data.[70] Even in clinic matters where there are fewer conceivable threats of malicious access, there is still a continuing obligation to reasonably protect client data from accidental or inadvertent disclosure, and from access by other third parties unrelated to the case—from a student's roommate, to the staff at a cloud storage company, to a run-of-the-mill hacker.

The clinical community centers respect for clients, their interests, and their dignity in its focus on training students to be thoughtful, reflective, client-centered lawyers, in representing oppressed communities, and in seeking to make positive social change.[71] While no group is a monolith, the community purports to incorporate those values in the attorney-client relationships formed through clinic work.[72] These commitments each reflect the centrality of basic human dignity not just in clinics but throughout the profession.[73] Upholding our values means not only practicing law in a way that protects client dignity, but fostering our students' commitment to the same. In these ways, we seek to practice what we preach.

Roughshod treatment of client data flies in the face of these commitments and betrays our core tenets. This may be best demonstrated through an analysis of our commitment to confidentiality more broadly. The duty of confidentiality is classically orientated around fostering open communication between lawyer and client,[74] as well as protecting a client's dignity and autonomy.[75] As Professor David

[70] What is reasonable, of course, may be informed by the severity of the risk of unauthorized access. *See infra* Part II.

[71] *See, e.g.*, DAVID A. BINDER, PAUL B. BERGMAN, PAUL R. TREMBLAY & IAN S. WEINSTEIN, LAWYERS AS COUNSELORS: A CLIENT-CENTERED APPROACH (4th ed., 2019); *see* Barry et al., *supra* note 15, at 12–16; ASS'N OF AM. L. SCHS., BYLAWS OF THE SECTION ON CLINICAL EDUCATION 1 (amended Jan. 4, 2022), https://www.aals.org/wp-content/uploads/2022/11/BYLAWS-Fall-2022-Clinical-Legal-Education.pdf ("The Section's work includes . . . building on deep-rooted pedagogical and community values that include a focus on social injustice."). R

[72] *See* Nina W. Tarr, *Clients' and Students' Stories: Avoiding Exploitation and Complying with the Law to Produce Scholarship with Integrity*, 5 CLIN. L. REV. 271, 293 (1998) ("The clinic clients . . . should be afforded the same integrity, privacy, dignity and right to self-determination as the medical patient.").

[73] *See* Robert K. Vischer, *How Do Lawyers Serve Human Dignity?*, 9 U. ST. THOMAS L.J. 222, 248 (2011) ("A commitment to human dignity compels lawyers to widen their gaze, to remember that law serves the well-being of the human person, and thus the person must remain at the center of their work.").

[74] *See* MODEL RULES OF PRO. CONDUCT r. 1.6 cmt. 2 (AM. BAR ASS'N, 2020) (noting that the confidentiality obligation "encourage[s clients] to seek legal assistance and to communicate fully and frankly with the lawyer even as to embarrassing or legally damaging subject matter").

[75] David Luban, *Lawyers as Upholders of Human Dignity (When They Aren't Busy*

Luban has noted, this is because "having human dignity means being an individual self who is not entirely subsumed into larger communities. Not only are we subjects of a story, it is our story, and human dignity requires that we not be forced to tell it as an instrument of our own condemnation."[76] In other words, the obligation of confidentiality is meant to ensure that by securing representation clients are not also waiving the choice to keep their information private. Surely most, if not all, clinical educators vigilantly protect client confidences stored in our memories and paper files. If true, that same vigilance should protect intangible client data, even when challenging.

More than that, we must model that vigilance for our students.[77] One value of clinical education is its capacity to inculcate students with an appreciation for client dignity and the need to treat clients with respect. We must help students to see why technology use relates to client dignity, to our ethical obligations, to best practices, and to what kind of lawyer they want to be.[78] Increasingly, our students "have never lived in a world without accessible technology, and they often use technology without a second thought."[79] Some students have accepted as a known risk that what they do online is rarely truly private, and they may be transferring that into their clinic work. When practicing law, our students cannot use technology thoughtlessly, particularly when social norms around technology fall short of an attorney's ethical obligations. It is incumbent on us to ensure students use technology thoughtfully and ethically, consistent with our mission.[80]

Of course, not all members of the clinical community are unaware of the need for ethical technology use. A set of proposed guidelines for clinical education written by J.P. "Sandy" Ogilvy and based on the work of a 1995 joint committee between the American Association of Law Schools (AALS) and the Clinical Legal Education Association (CLEA)[81] raised these exact questions with respect to technology. Professor Ogilvy included the following prompts as re-

Assaulting It), 2005 U. ILL. L. REV. 815, 830–38 (2005).

[76] *Id*. at 838.

[77] *See* Peter A. Joy, *The Ethics of Law School Clinic Students as Student-Lawyers*, 45 S. TEX. L. REV. 815, 840 (2004) ("Law school clinics that are model ethical law offices are ones where clinic faculty, staff, and students not only follow applicable ethics rules, but also discuss the ethical rules and issues they confront and the procedures in place to protect clients and fulfill their ethical obligations.").

[78] Mark Neal Aaronson, *We Ask You to Consider: Learning About Practical Judgment in Lawyering*, 4 CLIN. L. REV. 247, 249 (1998) ("Pedagogically, clinical legal education seeks not just to impart legal skills, but to encourage students to be responsible and thoughtful practitioners.").

[79] *See* Stringfellow Otey, *supra* note 9, at 226. R

[80] *Id.*

[81] J.P. "Sandy" Ogilvy, *Guidelines for the Self Evaluation of Legal Education Clinics and Clinical Programs*, 15 T.M. COOLEY J. PRAC. & CLIN. L. 1, 2–3 (2013).

lated to assessing a live-client clinic's facilities:

> 3.10.14. Does the program encourage the appropriate use of standard law office technology software?
>
> 3.10.14.1. Does the program have a technology-use policy that clearly informs all technology users in the clinical program of what they can do and cannot do while using e-mail, surfing the [internet], and using other law office systems?[82]

Some clinical programs have incorporated this guidance, and (as previously noted) more than a few scholars have addressed the role of technology in clinics.[83]

I suspect the main challenge is not that clinical educators do not think it is important to protect client data, but rather that they do not know how they are leaving it unprotected and, when confronted with these myriad challenges, are overcome by a feeling of how hard it will be to fix them. Learning and applying new technologies and law office policies will surely require adjustments, and may make law practice more difficult. Yet as a community, we consistently strive to hold ourselves to a standard of excellence. If excellence is our aspiration—and I think it ought to be—then we need to live up to it.

Moreover, many clinical faculty are "othered,"[84] and their programs under-resourced,[85] making pursuit of technology security potentially risky. Some protections incur costs, which could either draw on the limited funds a clinic already receives or reinforce the perception that clinics are more expensive than they are "worth."[86] Even no-cost interventions, like a policy to screen and shield confidential emails, could cause unsupportive administrators to question whether clinic-client representation is a liability to the university. In short, there are surely some clinical programs that are constrained from implementing security measures they otherwise might.

Whatever the reasons, it is time for the clinical community to get up to speed, to meet the moment, and to reasonably protect client

---

[82] *Id.* at 62.

[83] *See supra* notes 12–15 and accompanying text. R

[84] *See* Nina W. Tarr, *In Support of a Unitary Tenure System for Law Faculty: An Essay*, 30 WM. MITCHELL L. REV. 57, 70 (2003).

[85] While many institutions, and the ABA, have grown to recognize clinics as an integral and coequal component of legal education, there remain schools where clinics are not so treated. *See* Todd A. Berger, *Three Generations and Two Tiers: How Participation in Law School Clinics and the Demand for "Practice- Ready" Graduates Will Impact the Faculty Status of Clinical Law Professors*, 43 WASH. U. J.L. & POL'Y 129, 135 (2013) ("The significant expansion in the total number of law school clinics has not brought with it broad-based institutional legitimacy for clinical law professors.").

[86] Bryan L. Adamson, Calvin Pang, Bradford Colbert, Kathy Hessler, Katherine Kruse, Robert Kuehn, Mary Helen McNeal & David Santacroce, *Clinical Faculty in the Legal Academy: Hiring, Promotion and Retention*, 62 J. LEGAL EDUC. 115, 146 (2012).

data just as others in the legal profession do. The following section sketches out guidance for clinical educators seeking to do just that.

II. Ethical Imperatives

Client data is subject to a variety of obligations under the rules of professional conduct.[87] Governing ethics bodies have interpreted those rules to require reasonable measures to protect client data. In Section A, I discuss the reasonableness standard and how it is reflected in the duties relating to competence, confidentiality, safeguarding client property, and supervising nonlawyer assistants and subordinate lawyers. In Section B, I explore the ABA's guidance on implementing the reasonableness standard. This Part concludes with a brief review of state ethics opinions on the same topics.

Throughout, I use the phrase "clinic personnel" to refer to any person who must act in accordance with, or whose conduct lawyers must reasonably assure is compatible with, the rules of professional conduct.[88] This may include supervising attorneys, law students, staff assistants, paralegals, IT specialists, external service providers, or any other person whose activities the rules of professional conduct regulate. I use the phrase "clinic supervisors" to refer specifically to the lawyers ultimately accountable for violations of the rules of professional conduct.[89] This may include law professors, staff attorneys, fellows, or others who are serving as supervising attorneys under the rules of professional conduct and local student practice rules.[90] I use the phrase "clinic law firm" to refer to the collection of clinic supervisors, from one or more law school clinics, that make up a law firm for the purposes of the rules of professional conduct.[91] Depending on the structure created by the law school, each clinic could be its own law firm, groups of clinics could constitute different firms, or all clinics in the school could be one firm.[92] When I suggest that a clinic law firm should take certain steps, I refer to those within the organizational structure with authority to effect that change.[93]

---

87 I cite and apply the Model Rules of Professional Conduct in this analysis. Of course, individual jurisdictions apply their own codes of professional responsibility, and those rules may impose different or additional requirements.

88 *See* Model Rules of Pro. Conduct r. 5.3 (Am. Bar Ass'n, 2020).

89 *See id.* at rr. 5.2, 5.3.

90 Peter A. Joy & Robert R. Kuehn, *Conflict of Interest and Competency Issues in Law Clinic Practice*, 9 Clin. L. Rev. 493, 514–15 (2002).

91 *See* Model Rules of Pro. Conduct r. 1.0(c).

92 *See* Rovner, *supra* note 13, at 1014–17. R

93 In some circumstances, those with power to make needed change may not be part of the clinic law firm, may not agree that data security protections are necessary, and/or may not prioritize meeting clinics' needs. Clinic supervisors should seriously consider how to balance their ethical obligations in such circumstances. *See infra* Section III.G.

A. Applicable Rules of Professional Responsibility

Four primary ethical principles govern the storage and transmission of client data—the duties of competence, confidentiality, safeguarding client property, and supervising nonlawyer assistants.

1. Duty of Competence

The duty of competence[94] affirmatively requires attorneys to "keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology."[95] As a result, attorneys generally have an ongoing obligation to identify how technology contributes to the competent and effective practice of law, and also to understand the risks associated with its use. Of note, while other rules of professional responsibility have been interpreted to apply to client data, as discussed below, this rule contains the only explicit reference to technology.[96]

The requirement that lawyers stay abreast of changes to and risks associated with technology adds a dimension to the duty of competence that is critical for law school clinics. It requires clinic supervisors to stay up to date on these matters.[97] Not all lawyers—and not all clinic supervisors—have that level of familiarity with technology, its potential uses, or its potential misuses. Of course, computer technology is a science of its own, and understanding how legal tech works involves a steep learning curve, particularly for those who are not digital natives. Nonetheless, it is incumbent on each clinic supervisor, regardless of their background, to rise to the baseline on that curve.

2. Duty of Confidentiality

The duty to protect client confidences requires attorneys not to intentionally or inadvertently disclose information relating to the representation of a client.[98] The duty specifically requires attorneys to take "reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."[99] This obligation also extends to client

---

[94] MODEL R. OF PROF. CONDUCT r. 1.1.

[95] *Id.* at r. 1.1 cmt. 8.

[96] While it does not include an explicit reference to technology, Rule 1.6(c) was adopted specifically to reflect the changing landscape around technology and law practice. ABA COMM'N ON ETHICS 20/20, REPORT TO THE HOUSE OF DELEGATES 105A REVISED, at 4–5 (2012), https://www.americanbar.org/content/dam/aba/administrative/ethics_2020/20120808_revised_resolution_105a_as_amended.pdf.

[97] *See* Joy & Kuehn, *supra* note 90, at 560 ("A law clinic has the same duty to provide competent representation to clients as any other law firm or legal services provider."). R

[98] MODEL RULES OF PRO. CONDUCT r. 1.6(a) & (c).

[99] *Id.* at r. 1.6(c).

data.[100] The "reasonable efforts" standard "does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy."[101] Nor does it suggest that "a lawyer engages in professional misconduct any time a client's confidences are subject to unauthorized access or disclosed inadvertently or without authority."[102] Of course, because technology and the means to hack it change so rapidly, so does the definition of a "reasonable" expectation of privacy.

For that reason, it must become a routine part of law school clinic administration to stay abreast of evolving data storage technology and the cybersecurity challenges that come with it.[103] Over the course of the last three decades, expanded technology has created numerous new homes for client data outside a lawyer's mind and paper file.[104] Each of those new repositories—cloud storage, email, text messages, and so on—must secure client confidences through reasonable measures, just as would be expected for confidences stored in a filing cabinet at a law office. The risks of inadvertent disclosure of confidences on paper is fairly obvious—the attorney must take steps to ensure only authorized individuals can physically access those papers. This may involve storing paper files in locked filing cabinets, within a locked room. It also involves taking care with where the paper file goes—an attorney would avoid leaving the file alone in a coffee shop, or in the lobby.

Potential intrusions on client data are more numerous, and far less obvious than intrusions on paperwork. The discourse over client data confidentiality has tended to focus on inadvertent disclosure due to an attorney's mistake.[105] When email was first introduced to law

[100] *See infra* Section II.B.

[101] MODEL RULES OF PRO. CONDUCT r. 1.6, cmt. 18 & 19.

[102] ABA Formal Op. 477, *supra* note 8, at 4 n.11 (quoting ABA COMM'N ON ETHICS 20/20, REPORT TO THE HOUSE OF DELEGATES 105A (Aug. 2012), https://www.americanbar.org/content/dam/aba/administrative/ethics_2020/2012_hod_annual_meeting_105a_filed_may_2012.pdf). R

[103] 51 MASS. PRAC., PROFESSIONAL MALPRACTICE § 16.26 n.6 ("Given the seemingly endless and ever-accelerating pace of technology as it impacts all of modern life, including, law practice, it is apparent that what is 'reasonable' with respect to an attorney's knowledge and actions is changing all the time, effectively broadening the scope of the attorney's duty and standard of care in new and often unexpected ways.").

[104] Joseph W. Rand, *What Would Learned Hand Do?: Adapting to Technological Change and Protecting the Attorney-Client Privilege on the Internet*, 66 BROOK. L. REV. 361, 362 (2000) ("With the advent of online document repositories, cellular phones, handheld wireless computers, and instant messaging, lawyers have all sorts of new and exciting ways in which they can inadvertently breach their clients' confidences.").

[105] *See, e.g.*, Joseph L. Paller Jr., *"Gentlemen Do Not Read Each Other's Mail": A Lawyer's Duties upon Receipt of Inadvertently Disclosed Confidential Information*, 21 LAB. LAW. 247 (2006); David Hricik, *I Can Tell When You're Telling Lies: Ethics and Embedded Confidential Information*, 30 J. LEGAL PROF. 79 (2006); *see also* MODEL RULES OF PRO.

practice, ethics scholars warned of mistakes made by the attorneys themselves, like attaching the wrong file to an email or unintentionally transmitting privileged documents to third parties in electronic form.[106] This is a real risk, and it is important to continue to guard against it. As recently as August 2022, a lawyer representing Infowars radio personality Alex Jones in a defamation case involuntarily released his text messages and failed to retract the disclosure within the prescribed amount of time, resulting in the opposing party's attorneys using the messages to devastating effect at trial.[107] That lawyer was suspended from practice as a result.[108]

But the duty to protect a client's confidences extends beyond an attorney's active mistakes. An attorney can triple check every email and discovery response and still leave their client data open to third parties. Malware and hacking risk that third parties might obtain and misuse client data. If an off-site data storage provider receives a subpoena and is not obligated to contact the attorney, or unaware that it should do so before responding, client data might be released in response to the subpoena. Employees of off-site data storage providers might also have unfettered access to client data and, without the proper agreements, could mishandle it.

In short, the prospect that third parties might see, access, or misuse client data stored electronically requires attorneys to be particularly vigilant in protecting it.[109]

3. Duty to Safeguard Client Property

Client data also constitutes client property, which attorneys have a duty to protect and "appropriately safeguard[ ]."[110] While the Model Rules only explicitly refer to client funds and physical property, jurisdictions that have addressed the matter extend the obligation to client files and client data, as well. For example, in 1998, the D.C. Bar Legal

CONDUCT r. 4.4(b) & cmt. 2; ABA Comm'n on Ethics & Pro. Resp., Formal Op. 437 (2005).

106 *See generally* Anna G. Bruckner-Harvey & Amy M. Fulmer Stevenson, *Making a Wrong Turn on the Information Superhighway: Electronic Mail, the Attorney-Client Privilege and Inadvertent Disclosure*, 26 CAP. U. L. REV. 347 (1997).

107 *See* Elizabeth Williamson, *Alex Jones, Under Questioning, Is Confronted with Evidence of Deception*, N.Y. TIMES (Aug. 3, 2022), https://www.nytimes.com/2022/08/03/us/politics/alex-jones-trial-sandy-hook.html.

108 Joanna Slater & Rachel Weiner, *Alex Jones Lawyer Suspended for Sharing Medical Records of Sandy Hook Families*, WASH. POST (Jan. 6, 2023), https://www.washingtonpost.com/nation/2023/01/06/alex-jones-lawyer-suspension/.

109 *But see* Lanterman, *supra* note 19, at 18 ("[T]hose within the legal community are held to the highest standards of cybersecurity and discretion when it comes to handling data breaches and cyber events. Unfortunately, though, some attorneys seem to believe that the word 'reasonable' allows for a fairly low standard."). R

110 MODEL RULES OF PRO. CONDUCT r. 1.15(a).

Ethics Committee applied the rule on safekeeping client property to require attorneys to maintain client files for at least five years,[111] and applied the same principles governing client files in deciding that files may be kept solely electronically in 2010.[112] In 2013, the Ohio State Bar issued an informal opinion applying the rule to client data.[113] In 2018, the Massachusetts Supreme Judicial Court amended the state's Rules of Professional Conduct to specifically apply the principles of safeguarding client property to client files, "whether in physical or electronic form."[114]

4. Supervising Lawyers and Subordinate Nonlawyers

Finally, lawyers are generally responsible for the work of nonlawyer assistants, and partners or lawyers with managerial authority are charged with taking reasonable efforts to ensure that law firm employees' conduct is compatible with ethical rules.[115] The responsibility of lawyers to adequately supervise nonlawyer assistants and subordinate lawyers implicates each of the other professional obligations in two main ways: first, when the clinic law firm contracts with legal technology providers to support its law practice; and second, as clinic supervisors supervise clinic personnel, including law students.[116]

First, the rules of professional conduct require that lawyers secure reasonable and enforceable protections when contracting with outside vendors like cloud storage providers.[117] Rule 5.3 explicitly covers using "Internet-based services" to store "client information," which clearly includes off-site storage of client data.[118] Under the comments to the rule, lawyers must make "reasonable efforts" to ensure that the provider takes steps consistent with the lawyer's obligations.[119] What is reasonable depends on the provider's "education, experience and reputation[,] . . . the nature of the services involved[,] the terms of any arrangements concerning the protection of client information[,] and the legal and ethical environments of the jurisdictions in which the services will be performed, particularly with regard to confidentiality."[120] Typically, this requires lawyers to contract with third-party

111 D.C. Bar Legal Ethics Comm., Ethics Op. 283 (1998).

112 D.C. Bar Legal Ethics Comm., Ethics Op. 357 (2010).

113 *See, e.g.*, Pro. Comm. of the Ohio Bar Ass'n, Informal Opinion 2013-3 (2013) (comparing off-site data storage to off-site storage of paper files).

114 MASS. RULES OF PRO. CONDUCT r. 1.15A(a) (2018).

115 MODEL RULES OF PRO. CONDUCT rr. 5.2, 5.3.

116 *Id.* at rr. 5.2, 5.3.

117 *See* Douglas R. Richmond, *Watching Over, Watching Out: Lawyers' Responsibilities for Nonlawyer Assistants*, 61 U. KAN. L. REV. 441, 450 (2012).

118 MODEL RULES OF PROF. CONDUCT r. 5.3, cmt. 3.

119 *Id*.

120 *Id.*

technology providers to ensure they store and maintain client data consistent with the rules of professional conduct.[121]

Second, the rule requires the appropriate supervision of clinic personnel, including supervising their ethical use of legal technology. How the ethics rules and student practice rules treat clinic students varies by jurisdiction—some consider them akin to subordinate lawyers,[122] while others refer to them as "legal interns," though most if not all appear to allow clinic students to engage in the limited or supervised practice of law.[123] Additionally, some clinical law firms may employ the services of law students not enrolled in a clinic to participate in client matters as nonlawyer assistants (either as research assistants or to conduct other permissible tasks). Either way, clinic supervisors are ethically required to ensure that law students in clinics follow the rules of ethics.[124] Moreover, student practice rules typically make explicit the supervising attorney's obligation to ensure their students' ethical practice, or at least that the students must practice under their supervision.[125] This translates to a requirement that clinic supervisors adequately train students on each of their ethical obligations, including how to ethically use legal technology.[126] Of course, the obligation extends not only to law students but also to any nonlawyer to whom clinic supervisors delegate work governed by the rules of professional conduct. That could include staff assistants who provide clerical support to clinics, paralegals or legal interns who do work within the clinic law firm, or other nonlawyers who have access to client data.

B. The ABA Standing Committee on Ethics and Professional Responsibility

In 2017, the ABA Standing Committee on Ethics and Professional Responsibility issued Formal Opinion 477, which lays out updated guidance on the "reasonable efforts" standard governing confidentiality of client data.[127] As the opinion notes, "[w]hat constitutes reasonable efforts is not susceptible to a hard and fast rule, but rather is contingent upon a set of factors. In turn, those factors depend

121 *See infra* Appendix A.

122 MODEL RULES OF PRO. CONDUCT r. 5.2; *see also* Joy, *supra* note 77, at 832 ("The language in most jurisdictions' student practice rules explicitly or implicitly supports the conclusion that a student-lawyer should be treated as a lawyer for ethics purposes."). R

123 *See* Joy, *supra* note 77, at 832. R

124 *Id.* at 834.

125 *Id.*

126 *See* Boonin & Herrera, *supra* note 15, at 138; Stringfellow Otey, *supra* note 9, at 224–28. R

127 *See* ABA Formal Op. 477, *supra* note 8. R

on the multitude of possible types of information being communicated . . ., the methods of electronic communications employed, and the types of available security measures for each method."[128] As a result, the Committee imported a standard announced in the ABA Cybersecurity Handbook to define "reasonable efforts" in the context of client data:

> [The reasonable efforts standard] rejects requirements for specific security measures (such as firewalls, passwords, and the like) and instead adopts a fact-specific approach to business security obligations that requires a "process" to assess risks, identify and implement appropriate security measures responsive to those risks, verify that they are effectively implemented, and ensure that they are continually updated in response to new developments.[129]

In short, because technology is ever-changing, the ABA committee declined to offer a specific set of standards, instead encouraging lawyers to create a review process of its technology use as technology and threats evolve.[130]

Without announcing a specific standard, the Opinion did name seven guiding considerations for safeguarding client data through technology use. These guidelines apply with varying degrees of force and concern to different clinic types, but they are each essential in structuring clinic-wide technology policy.

1. Understand the Nature of the Threat

Clinics handling particularly sensitive information on behalf of a client are expected to take extra care to prevent unauthorized access or disclosure. Some client data is more sensitive and, therefore, more likely to attract infiltration or attempted theft.[131] Matters involving "industrial design, mergers and acquisitions or trade secrets, . . . healthcare, banking, defense[,] or education" are examples of high-risk client data.[132] This could apply to intellectual property clinics, medical-legal partnership clinics, securities clinics, policy clinics, or other clinics representing clients with, or otherwise handling, particularly sensitive information. The Opinion stops short of specific recom-

---

[128] *Id.* at 4.

[129] *Id.* (quoting JILL D. RHODES & VINCENT I. POLLEY, THE ABA CYBERSECURITY HANDBOOK: A RESOURCE FOR ATTORNEYS, LAW FIRMS, AND BUSINESS PROFESSIONALS 48–49 (2013)).

[130] *See* ABA Formal Op. 477, *supra* note 8, at 4 n.13 ("[T]echnology is changing too rapidly to offer [detailed] guidance and . . . the particular measures lawyers should use will necessarily change as technology evolves and as new risks emerge and new security procedures become available.") (quoting ABA COMM'N ON ETHICS 20/20, *supra* note 102, at 5). R R

[131] *See* ABA Formal Op. 477, supra note 8, at 5. R

[132] *Id.*

mendations, but notes that "greater effort is warranted."[133]

2. *Understand How Client Confidential Information Is Transmitted and Where It Is Stored*

Clinic supervisors must understand how their clinic's legal technology works—not only how it can be used day-to-day, but where client data and protected communications are generated and stored. "Every access point is a potential entry point for a data loss or disclosure."[134] As a result, clinic supervisors must be able to identify each way in which client data or clinic technology can be accessed, so that they can take reasonable steps to prevent misuse. This does not require a technical or scientific understanding of how the technology works; clinic supervisors almost certainly do not need to know what code cloud-based platforms use or how that code allows the web-based system to function. However, the duty does require that "each access point . . . be evaluated for security compliance."[135] Obtaining information like this allows clinic law firms to assess the risks and potential consequences, if any, of using the technology, and chart a way to use the technology while reasonably protecting client data.[136]

This guidance embodies what it means to be "competent" around technology, and is one of the greatest potential risks in clinic technology use.[137] Some clinic supervisors may find themselves taking on faith that, by employing a widely-used technology like Google Drive or Microsoft Outlook, they will benefit from reasonable protections.

---

133 *Id.*

134 *Id.* at 6.

135 *Id.* Representatives from case management software providers can likely offer information on where and how firm data is stored, as well as proof of security testing or other formal assurances about the security of their data and systems upon request.

136 For example, if a clinic uses a cloud-based case management system like Clio, then clinic supervisors must know how Clio secures client data and how clinic personnel, and Clio personnel, could misuse that system in a way that risks inadvertent disclosure, access, or data loss. The clinic law firm would need to identify that Clio stores client data on cloud-based servers and consider the risks cloud storage poses to that data. *See infra* Section III.A.2; *see also infra* Appendix A. The clinic law firm would also learn that Clio is a Canadian company whose terms of service are subject to the laws of British Columbia and Canada and that, without express agreement, their client data could be stored outside the United States. *See North American Terms of Service*, CLIO, https://www.clio.com/tos/ (Dec. 26, 2021). Storage on servers in Canada may well comply with ethical requirements, so long as the jurisdiction in which the data is stored confers an expectation of privacy at least as stringent as that conferred by United States law. *See infra* note 182 and accompanying text. And the clinic law firm would need to consider how clinic personnel will access Clio and how they will use Clio to protect any information stored there (by learning it can store client documents on its cloud-based servers and, for example, using Clio Drive to avoid downloading work product directly to personal devices). *Secure, Seamless File Management with Clio Drive*, CLIO, https://www.clio.com/web/drive/ (last visited Jan. 29, 2023). R

137 MODEL RULES OF PRO. CONDUCT r. 1.1 cmt. 8 (AM. BAR ASS'N, 2020).

To the contrary, standard user agreements with these vendors typically omit the kind of protections that would reasonably protect client data.[138] The risk of this assumption may be even greater when the university provides the service to employees and students, rather than the clinic law firm specifically. In short, clinic supervisors cannot simply take it on faith that this technology will be "good enough."

Indeed, that some in the profession use technology but do not understand its potential for misuse also demonstrates the need to incorporate technology ethics into our pedagogy.[139]

3. Understand and Use Reasonable Electronic Security Measures

Clinic supervisors must understand, and clinic law firms must employ, widely used security measures to protect client data. While the ABA Opinion declines to lay out any formal requirements, it makes abundantly clear that some measures that are "routinely accessible and reasonably affordable or free" are as close to required as can be.[140] First, clinics must ensure client data is accessed through secure methods, either secure Wi-Fi, VPNs, or secure portals.[141] Second, devices used to store or access client data should have "unique complex passwords, changed periodically," as well as "firewalls" and "anti-Malware," "anti-Spyware," and/or "Antivirus" software.[142] Third, such devices must also regularly update their standard security features.[143] The Opinion also describes other tools that might be available to clinics, including multi-factor authentication for accessing firm systems and encryption.

Notably, the Opinion strongly discourages reliance on "deleting" client data from devices as a means to prevent disclosure or access. As the Opinion notes, most "deleted" data can be recovered, suggesting that client data might "[*n*]*ever* be stored in an unencrypted environment."[144] Clinic supervisors must be particularly mindful of this guidance when permitting clinic personnel to use personal devices for client-related work without a secure remote access tool.[145]

---

138 *See infra* Part III.

139 *See* Boonin & Herrera, *supra* note 15, at 117–21; *see also* Peter A. Joy, *The Law School Clinic as a Model Ethical Law Office*, 30 WM. MITCHELL L. REV. 35 (2003). R

140 *See* ABA Formal Op. 477, *supra* note 8, at 6. R

141 *Id.*

142 *Id.*

143 *Id.*

144 *Id.* at 7 (emphasis in original).

145 *See Remote Access*, TECHOPEDIA.COM (Dec. 20, 2016), https://www.techopedia.com/definition/5553/remote-access ("Remote access refers to the ability to access a computer, such as a home computer or an office network computer, from a remote location. This allows employees to work offsite, such as at home or in another location, while still having access to a distant computer or network, such as the office network.").

4. Determine How Electronic Communications About Client Matters Should Be Protected

Clinic law firms must determine what level of protection to afford electronic communications like emails and text messages, both to clients and third parties. Generally, communications that do not "warrant extra security"[146] are "routine" and do not require additional protections. However, the Opinion also notes that additional protections might be needed where clients use devices or communication methods that could be accessed or controlled by third parties.[147] For example, this heightened standard might apply if a family law clinic represents a client in a divorce and the opposing party might have their password, or if a client shares an email account with a family member.[148] Another example comes when the lawyer learns the client is accessing their emails on devices that do not confer a reasonable expectation of privacy, like employer-owned computers. In those circumstances, the lawyer has a duty to "caution the client not to do so," and should consider what, if any, alternative measures might be taken to preserve the confidentiality of email communications.[149]

For communications that do require heightened security, clinic law firms should consider using a case management system's secure document-sharing portal, or email encryption, which is typically available in most mainstream cloud-based email platforms. Some secure case management platforms allow sharing encrypted documents through an accessible link, which could replace attaching documents directly to an email. Encrypting emails ensures that the contents of the email are scrambled and cannot be accessed maliciously. Encrypting emails can also, however, make it more challenging for the recipient to open the email if they are not familiar with or do not have access to the application needed to do so. However, where clients do not have flexibility in electronic communications, clinics should consider explicitly counseling the client on the risks of insecure communication and coming to a written agreement about their preferences, in light of the risks.[150]

---

146 *See supra* Section II.B.1.

147 *See* ABA Formal Op. 477, *supra* note 8, at 8. R

148 *Id.* at 7 & n.18.

149 *See* ABA Comm. on Ethics & Pro. Resp., Formal Op. 459, 4 n.7 (2011). The ABA has suggested that if the client continues accessing confidential emails on employer-owned devices after the attorney has informed the client of the risks of doing so, the lawyer should "cease sending messages even to personal e-mail addresses." *Id*. In subsequent guidance, the ABA qualified that additional protections, like encryption, may alleviate the concern. ABA Formal Op. 477, *supra* note 8, at 7 & n.17. It may be that other reasonable protections would suffice, particularly where the client's circumstances offer no alternative means to communicate with their lawyer. R

150 *See infra* Section III.G.

5. Label Client Confidential Information

The Opinion specifically advises lawyers to use a disclaimer marking electronic communications as privileged and confidential and warning inadvertent recipients that it is intended as such.[151] Clinics should ensure that faculty, staff, and students all use the same disclaimer on such communications. Sample language for such a disclaimer can be found in Appendix B.

6. Train Lawyers and Nonlawyer Assistants in Technology and Information Security

Perhaps most critically for clinics, the Opinion requires a series of steps when supervising "nonlawyer assistants"—in clinics, our students and staff. Of note, the Opinion lists a series of steps lawyers "must" take, in contrast to those lawyers "should" take with respect to other guidelines.

Clinics must "establish policies and procedures . . . in the use of reasonably secure methods of electronic communications."[152] Moreover, clinic law firms must "periodically train" clinic personnel on how to securely use legal technology and securely treat client data.[153] It is incumbent on clinic supervisors to "follow up to ensure these policies are being implemented."[154] Finally, clinic supervisors must "periodically reassess and update" the policies to ensure reasonableness as technologies and risks change.[155] As a result, clinic supervisors must consider how to assess compliance with clinic law firm technology policy, and whether and how to evaluate law student compliance with that policy when awarding a grade.

7. Conduct Due Diligence on Vendors Providing Communication Technology

Legal technology involving cloud storage of client data also invokes the requirements of Rule 5.3. Those providers are "nonlawyer assistants" charged with storing and/or transmitting client data. Just as with any other outside party retained to do legal work, clinics must perform "due diligence" to ensure the vendor will act compatibly with the lawyer's ethical duties.[156] This could include vetting the provider's security protocols, adopting confidentiality agreements, ensuring there are no positional or imputed conflicts with clinic clients, and

[151] *See* ABA Formal Op. 477, *supra* note 8, at 8. R
[152] *Id.*
[153] *Id.*
[154] *Id.* at 8–9.
[155] *Id.*
[156] *Id.* at 9 (citing ABA Comm. on Ethics & Pro. Resp., Formal Op. 451 (2008)).

making enforceable any terms around violation of agreements regarding treatment of clinic client data.[157]

* * *

Together, these guidelines suggest two conclusions. First, many clinics are falling short of ABA guidance for proper protection of electronic client data—particularly the nearly half of clinics that offer no written policies or training on data security to their students.[158] Second, creating such policies is both possible and necessary to protect clinic clients from data breaches and to protect clinic personnel from ethical violations.

In addition to the guidance of the ABA and Model Rules, state bar ethics commissions have issued additional jurisdiction-specific guidance. Jurisdictions offer varying degrees of specificity to outline what kinds of protections will make an attorney's or law firm's efforts reasonable under this standard. Some jurisdictions focus on the lawyer's obligation to ensure that providers that store client data "will handle the storage and security of the data . . . [and] abide by a confidentiality agreement in handling the data," on top of a "continuing duty to stay abreast of appropriate security safeguards that should be employed."[159] Others provide a more comprehensive list of factors to be considered in evaluating reasonableness of third-party vendors, security precautions, and technology safeguards.[160] In one of the most robust ethics opinion on the topic, the Pennsylvania Bar Association Committee on Legal Ethics and Professional Responsibility detailed a comprehensive set of measures lawyers and law firms can take to ensure the reasonable protection of client data.[161] Clinics should consult the relevant ethics opinions for each jurisdiction in which their clinics practice law to ensure compliance. Most jurisdictions have issued ethics opinions with guidance on these questions.[162]

---

157 *Id.* at 9.

158 *See* Boonin & Herrera, *supra* note 15, at 131–32. R

159 Ala. St. Bar, Ethics Op. 2010-02, at 16–17 (2010).

160 *See, e.g.*, State Bar of Cal. Standing Comm. on Pro. Resp. & Conduct, Formal Op. 179, at 3–6 (2010).

161 Pa. Bar Assoc. Comm. on Legal Ethics & Pro. Resp., Formal Op. 200, at 7-10 (2011).

162 *See, e.g.*, Ala. State Bar Off. of Gen. Couns., Op. 02 (2010); Alaska Bar Assoc. Ethics Op. 2014-3 (2014); State Bar of Ariz. Ethics Op. 05-04 (2005); State Bar of Ariz. Ethics Op. 07-02 (2007); State Bar of Ariz. Ethics Op. 09-04 (2009); State Bar of Cal. Standing Comm. on Pro. Resp. & Conduct, Ethics Op. 179 (2010); Colo. Bar Assoc. Ethics Comm., Formal Op. 90 (revised 2018); Conn. Bar Assoc. Pro. Ethics Comm., Informal Op. 99-52 (1999); Conn. Bar Assoc. Pro. Ethics Comm., Informal Op. 2013-07 (2013); D.C. Bar Legal Ethics Comm., Ethics Op. 341 (2007); D.C. Bar Legal Ethics Comm., Ethics Op. 357 (2010); Fla. Bar Pro. Ethics Comm., Ethics Op. 10-2 (2010); Fla. Bar Pro. Ethics Comm., Ethics Op. 12-3 (2012); Ill. State Bar Assoc., Pro. Conduct Advisory Op. 16-06 (2016); Iowa State Bar

III. A Roadmap for Reasonable Clinic Data Privacy Policies

As a practical, ethical, and pedagogical matter, law school clinics must come to comply with these standards. This section lays out a blueprint for a clinic technology use policy. I identify the questions that clinic law firms must answer, and suggest options that would advance ethical compliance on each. Finally, I suggest sample language for agreements with technology service providers and a sample technology use policy for clinic personnel. By adopting these measures, law school clinics can ensure that they meet their ethical obligations and afford clinic clients the dignity and protection they deserve, and that the rules of professional conduct require. Of course, not all clinics will have the funding, staffing, or institutional support to implement every recommendation. Clinic law firms should implement those measures that are feasible under the circumstances, and that rise to meet the reasonableness threshold.[163]

A. Where Does the Data Live and Is It Secure? Cloud Storage, Case Management Systems, and Local Servers

Clinic law firms must first identify what platforms the clinic will use to store client data, and then take steps to ensure each of those platforms will reasonably protect the data. Clinics could choose to

Assoc. Comm. on Ethics & Prac. Guidelines, Ethics Op. 11-01 (2011); Ky. Bar Assoc., Ethics Op. KBA E-437 (2014); La. State Bar Assoc., Public Op. 19-RPCC-021 (2019); Me. Bd. of Overseers of the Bar Pro. Ethics Comm., Enduring Ethics Op. 194 (2008); Me. Bd. of Overseers of the Bar Pro. Ethics Comm., Enduring Ethics Op. 207 (2013); Mass. Bar Assoc., Ethics Op. 00-01 (2000), Mass. Bar Assoc., Ethics Op. 05-04 (2005), Mass. Bar Assoc., Ethics Op. 12-03 (2012); State Bar of Mich., Ethics Op. 381; Mo. Bar Legal Ethics Couns., Informal Advisory Op. 2018-09 (2018); Neb. State Bar Assoc. Ethics Advisory Comm., Ethics Advisory Op. 19-01 (2019); State Bar of Nev. Standing Comm. on Ethics & Pro. Resp., Formal Op. No. 33 (2006); N. H. Bar Assoc., Ethics Comm., Advisory Op. 2012-13/04 (2013); N.J. Advisory Comm. on Pro. Ethics, Op. 701 (2006); N.Y. State Bar Assoc. Comm. on Pro. Ethics, Ethics Op. 709 (1998); N.Y. State Bar Assoc. Comm. on Pro. Ethics, Ethics Op. 842 (2010); N.C. State Bar Ethics Comm., 2011 Formal Ethics Op. 6 (2012); Ohio Bd. of Pro. Conduct, Advisory Op. 2017-05 (2017); State Bar Assoc. of N.D. Ethics Comm., Op. 99-03 (1999); Or. State Bar, Formal Op. 2011-188 (revised 2015); Pa. Bar Assoc. Comm. on Legal Ethics & Pro. Resp., Op. 2011-200 (2011); Bd. of Pro. Resp. of Tenn. Sup. Ct., Formal Ethics Op. 2015-F-159 (2015); Pro. Ethics Comm. for the State Bar of Tex., Op. 648 (2015); Pro. Ethics Comm. for the State Bar of Tex., Op. 680 (2018); Vt. Bar Assoc., Advisory Ethics Op. 2010-6 (2010); Va. State Bar Standing Comm. on Legal Ethics, Legal Ethics Op. 1872 (2013); Wash. State Bar Assoc. Comm. on Pro. Ethics, Advisory Op. 2215 (2012); State Bar of Wis. Pro. Ethics Comm. Op. EF-15-01 (amended 2017).

[163] Indeed, in adopting Rule 1.6(c), the ABA's Commission on Ethics 20/20 noted that what is reasonable depends on various factors unique to each lawyer-client relationship, including "the cost of the safeguards and the sensitivity of the information, recogniz[ing] that each client, lawyer or law firm has distinct needs and that no single approach should be or can be applied to the entire legal profession." Report of the ABA Commission on Ethics 20/20, *supra* note 20, at 8. R

store client data on local servers or on remote servers using cloud storage. Clinics should not, however, allow client data to be stored directly on students' or faculty's devices without carefully considering and addressing the risks. I discuss each in turn.

1. Prohibiting Storage on Personal and University Devices

Clinics should not permit client data to be stored directly on personal devices, absent circumstances that render the alternatives described below unavailable. Students and faculty may need (or prefer) to work on client matters outside of the clinic's physical space. Indeed, during the pandemic, such work was both common and necessary.[164] However, client data stored on clinic personnel's personal devices becomes open to all manner of possible breaches. The device may be hacked or infected with a virus, causing client data to be lost or accessed by third parties. The data may be available to third parties who access the device, with or without an individual clinic personnel's consent.[165] And, the data may remain on the device after clinic personnel (particularly law students) leave the clinic law firm, meaning the clinic law firm loses control of that data and the ability to safeguard it.

If the clinic law firm permits storage of any client work on personal devices, it should require that clinic personnel encrypt the hard drive on the device. Encrypting a hard drive means that data stored on that hard drive can only be accessed by someone with a specific password to decrypt the hard drive each time it is accessed (in addition to any other password on the device).[166] Hard drive encryption is available for most laptop computers at no cost, making this a particularly effective measure for clinic law firms without the funding for extensive change.[167]

The clinic law firm should create procedures for securely deleting any client data that had been stored on a personal device. At a mini-

164 *See* Boonin & Herrera, *supra* note 15, at 109–10. R

165 *See* Sisk & Halbur, *supra* note 14, at 1287 ("[T]he acceptable use by lawyer and client of computer technology, e-mail, and other electronic files for professional matters is based on the assumptions that: the network on which the computer system exists is truly secure and private, that no stranger to the attorney-client relationship has a right of access to the content of electronic files, and that the supporting technology staff have been instructed about confidentiality and are answerable to the lawyer or the client who creates the documents or transmits the confidential communication."). R

166 Margaret Rouse, *Hard Drive Encryption*, TECHTARGET.COM, https://www.techtarget.com/searchenterprisedesktop/definition/hard-drive-encryption (last visited Jan. 28, 2023).

167 For example, Mac users may use File Vault, *see Use FileVault to Encrypt Your Mac Startup Disk*, APPLE, https://support.apple.com/en-us/HT204837 (last visited Jan. 28, 2023), and Windows users may use BitLocker, *see BitLocker*, MICROSOFT, https://learn.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-overview (last visited Jan. 28, 2023).

mum, at the end of their time in the clinic law firm, clinic personnel must be required to delete all client data from their device (including their downloads folder) and to empty their recycling bin. Even if clinic personnel are required to delete client files, that data is likely still recoverable and accessible.[168] Notably, some "file-shredding" programs can overwrite the empty space that allows files to be recovered, significantly decreasing the risk that it will be accessible.[169] Such programs may be important pieces to a reasonable data privacy policy, particularly in instances where a document must be downloaded to a device for any reason (for example, where multiple PDFs need to be combined, or a document needs to be attached to an email). Clinic law firms should seriously consider how to most effectively implement such a process.

Clinics should also take care before permitting client data to be stored on university-owned devices. Data ownership becomes murky when it comes to devices and accounts owned by the university.[170] Some university privacy policies explicitly permit university personnel to access electronic data on university devices, which presents serious risks to the confidentiality of client data stored on those devices.[171] Clinics must thoroughly review university privacy policies to determine whether they are using university devices in a way that opens client data up to access by university employees outside the clinic law firm, and adjust their technology use policy accordingly.[172]

2. Clinic-Managed Cloud Storage and Collaborative Tools

To avoid the risks of storing client data directly on devices, clinics should explore secure cloud-based storage platforms and collaborative tool suites.[173] There are two primary cloud-based formats for storing clinic client data: commercial cloud storage providers and commercial case management systems designed for use in legal practice.[174] Both

[168] Chris Hoffman, *Why Deleted Files Can Be Recovered, and How You Can Prevent It*, How-to Geek (Jun. 8, 2018), https://www.howtogeek.com/125521/htg-explains-why-deleted-files-can-be-recovered-and-how-you-can-prevent-it/.

[169] *Id.*

[170] *See* Sisk & Halbur, *supra* note 14, at 1295–98 (reviewing various forms of university privacy policies regarding electronic data and communications). R

[171] *Id.* at 1297–98.

[172] *See infra* Section III.C.

[173] As of the time of this writing, common examples include Box, Microsoft365 Suite, and Google Suite. The further the reader is from the date of this publication, the more likely it is that these services are available through other providers or have been supplanted by updated technologies.

[174] Many web-based email providers also use cloud storage. Because email raises additional concerns regarding communications to third parties, I treat that topic separately for the purposes of this Article. *See infra* Section III.D.

store client data on remote servers outside the direct control of the clinic law firm, and therefore require particular treatment to ensure the confidentiality and security of client data. Clinic law firms must choose which cloud-based providers to use to store client data and create an enforceable agreement to ensure the data is reasonably protected.

Many law school clinics currently have access to, and use, commercial cloud storage providers like Box, Dropbox, Google Drive, and OneDrive.[175] These platforms present more complex challenges when used in the clinic law firm setting, as compared to other law firms. Typically, the university or law school contracts with one of those, or similar, providers to offer all students access to cloud storage.[176] However, clinic law firms should not use university-sponsored cloud storage if the written agreement with the cloud storage provider does not contain provisions that reasonably protect client data. For similar reasons, clinic law firms should not store client data on remote learning management systems like Blackboard or Canvas, which are likely accessible to a wider swath of university personnel such as IT staff, administrators, and others.

One option available to clinics is to work within the procurement process of the university or law school, as applicable, to amend existing contracts or to renegotiate the terms when they are up for renewal. Another is for the clinic law firm to enter a separate contract as a subdivision of the law school or university, which may still require approval of the appropriate contracting authority or procurement process. Either way, it is imperative that cloud storage agreements contain enforceable obligations to protect client data.[177]

Many law school clinics also use case management systems like Clio to store client information. Some law schools pay for case management systems, while others contract with no-cost alternatives.[178] Many for-cost case management systems offer additional features or customization that may assist clinical faculty in their pedagogy, as well as meeting ethical obligations.[179] Using a case management system to

[175] *See* Boonin & Herrera, *supra* note 15, at 127. R

[176] Some universities may include law schools in cloud storage contracts along with all other divisions of the university. Some law schools may contract for cloud storage for law students separate from other divisions of the university.

[177] *See infra* Appendix A.

[178] *See Get Clio in Your Classroom*, CLIO, https://www.clio.com/partnerships/academic-access/ (last visited Jan. 28, 2023).

[179] For example, as of the date of this writing, Clio does not allow for complete walling between clinics and allows any user in the firm to access data linked to a contact, rather than a matter. Clinic law firms that rely on walling to operate as one firm and avoid potential conflicts may fall short of their ethical obligations if a conflict arises and the conflicted student or employee has access to the client data with respect to which they have a conflict.

store client data is an effective way to shield it from unwanted intrusion. Most commercial case management systems are now cloud-based, and come with security features that match prevailing data-privacy norms.[180] Because these systems are designed to handle client data, they are more likely to be structured to reasonably protect it.

That said, law school clinics must review and supplement contracts with case management providers to ensure they comply with ethical standards. Boilerplate contractual language offered by case management providers may omit some terms or frame them in a way that does not match the structure of law school clinics.[181] Where standard user agreements fall short, case management system providers may be open to including additional terms in an addendum.

For both cloud storage and case management systems, clinic law firms should ensure the contract providing the service includes terms that match the ethical obligations described above. For example, the contract should certify that the cloud storage or case management system provider uses best practices in data security and will take reasonable measures to maintain them. It should clearly identify that the provider gains no ownership or security interest in the client data, has no right to "mine" the data for information, sell the data, or use it for any other purpose. It should require that client data be stored in the United States, or in geographic areas with privacy laws at least as rigorous as the United States'.[182] It should specify the obligation to keep the data secure and confidential, and provide a system to report intrusion into, loss of, or requests for client data. Specifically, the contract should specify an employee at the clinic law firm to contact in the event data is damaged, wrongfully obtained, or requested by subpoena. Finally, it should outline a process for retrieving client data in the event the provider ceases operations or the clinic law firm no longer wishes to contract with it. Each of these measures ensures that the clinic law firm has taken reasonable steps to protect the client

See MODEL RULES OF PRO. CONDUCT rr. 1.7, 1.8, 1.9, 1.10 (AM. BAR ASS'N, 2020).

180 *See, e.g.*, *Clio's Industry-Leading Security*, CLIO, https://www.clio.com/security/ (last visited Jan. 28, 2023).

181 For example, as of the date of this writing, Clio's terms of service include many, though not all, of the recommended provisions. Currently it does not guarantee in which jurisdictions the data will be stored, nor does it explicitly state that Clio gains no ownership interest in client data. *See North American Terms of Service*, CLIO, https://www.clio.com/tos/ (Dec. 26, 2021).

182 This reflects the view that what is "reasonable" depends upon the expectation of privacy afforded to client data as defined by United States law. *See, e.g.*, Pa. Bar Assoc. Comm. on Legal Ethics & Pro. Resp., Op. 2011-200 (2011) ("If by agreement, the data are hosted outside of the United States, the law firm must determine that the hosting jurisdiction has privacy laws, data security laws, and protections against unlawful search and seizure that are as rigorous as those of the United States and Pennsylvania.").

data, while allowing the firm to utilize needed cloud storage. Suggested contractual language is in Appendix A.[183]

Clinics should also clearly and unambiguously prohibit students from using personal cloud storage or collaborative tools to do client work. Client data stored on personal cloud storage accounts do not benefit from the kind of protections the rules of professional conduct require. For example, Google Drive files may be accessed by "Google employees, contractors, and agents," which may violate the confidentiality obligation.[184] Similarly, the policy offers no assurances with respect to notifying users if their information is accessed by anyone outside of Google, on the nature of data backups, or on the geographic location of the servers storing the data.[185] Because students are very unlikely to have secured the additional protections recommended above and in Appendix A, clinic law firms risk that client data stored on those personal clinic personnel accounts will be treated improperly or accessed inappropriately. For that reason, client data should only be stored on cloud storage providers approved by the clinic law firm, with the benefit of contractual protections.

3. Local Servers

Local servers bring the supervision of nonlawyer assistants much closer to home by allowing clinic personnel to administer the servers in the law school. These servers can also be burdensome to maintain, as they require more in-house work to manage and require additional tools to access remotely.

If clinics opt to use local servers, any staff managing the servers must be properly trained on the obligation to keep the data confidential and should sign confidentiality agreements to that effect. Clinics should also protect local servers with firewalls and standard anti-malware, anti-spyware, and anti-virus software.[186] Clinics should create authentication protocols for accessing the servers directly or remotely, and create a system to trace who has accessed client data. If possible, clinics should retain outside services to run penetration testing[187] to ensure the security of their servers.

---

183 *See also* W. Kuan Hon, Christopher Millard & Ian Walden, *Negotiating Cloud Contracts: Looking at Clouds from Both Sides Now*, 16 STAN. TECH. L. REV. 79, 92–125 (2012).

184 *Google Privacy and Terms: Privacy Policy*, GOOGLE, https://policies.google.com/privacy (Dec. 15, 2022).

185 *Id.*

186 *See* ABA Formal Op. 477, *supra* note 8, at 6. R

187 "A penetration test, also known as a pen test, is a simulated cyber attack against your computer system to check for exploitable vulnerabilities." *Penetration Testing*, IMPERVA, https://www.imperva.com/learn/application-security/penetration-testing/ (last visited Jan. 28, 2023).

Hosting client data on local servers also requires that clinic supervisors, staff, and students have access to the server. One option is to only permit supervisors, staff, and students to access the network locally, when they are connected to the network at the clinic's physical location. This option is far less practicable, as remote lawyering has become more central to law clinic practice during the pandemic.[188] Alternatively, clinic attorneys and students can access the server remotely using a VPN or VDI. VPN and VDI technology can impose additional costs and upkeep, which clinics should consider in deciding which option best meets budgetary and logistical goals. Less sophisticated versions of these tools can also be slow-moving and cause delays. VDI technology, however, also allows clinic personnel to access cloud-based storage, avoiding some of the risks of using web browsers on personal devices and allowing users to download and upload documents with client data in the secure environment of the VDI.

B. How Will Clinic Personnel Access and Transmit Client Data? Use of Personal Devices and Communication Tools

1. Personal Computers, Tablets, and Similar Devices

Initially, clinic law firms should be clear with clinic personnel which devices they may and may not use to access client data. The clinic law firm should train clinic personnel to never access client data on public computers (such as at a library) or computers owned by others (a family member or acquaintance, or an employer outside the law school).[189] Clinic law firms should also ensure that clinic personnel take reasonable precautions when using university and personal devices to access client data remotely.[190] As noted above, client data should generally not be stored directly on personal devices.[191] However, personal devices can be safely used to remotely access client data with the proper precautions.

First, any devices used to access client data should have updated anti-virus and firewall software that come standard with laptop computers. Second, any device used to access client data should be password protected to ensure it cannot be accessed by third parties. Third, clinics should train students to only access client data on secure Wi-Fi

[188] *See* Boonin & Herrera, *supra* note 15, at 109–10. R

[189] Clinic law firms should be particularly vigilant in training law students who are engaged in legal or non-legal employment outside of the clinic. *See* Joy & Kuehn, *supra* note 90, at 511 ("It is not unusual for law students admitted to practice under student practice rules as student-lawyers also to work concurrently in nonlawyer roles such as law clerks in law firms or government offices."). R

[190] *See* Sisk & Halbur, *supra* note 14. R

[191] *See supra* Section III.A.1.

networks, and never on public or unprotected Wi-Fi.[192]

Clinic personnel should create strong passwords for each technology account used to access client data, including case management software, collaborative and document storage tools, and email. Passwords that are longer, more complex, and randomly generated are less susceptible to being hacked.[193] For example, passwords that use actual words rather than random assortments of letters and numbers are more susceptible to "dictionary attacks," where a program attempts to use common words or phrases to hack the password.[194] Similarly, passwords or personal identification numbers (PINs) that use numbers associated with the user (birthdays, addresses, etc.) are more susceptible than those that use randomly generated numbers or letters.[195]

Clinic law firms should require passwords to be a minimum number of eight characters or longer (the longer, the more secure[196]), require that the password include at least one capital letter, lowercase letter, number, and special character, and include at least some combination of letters that is not a dictionary word.[197] Of course, clinic personnel must be able to remember their password without writing it down or storing it electronically, which also creates a risk of malicious access.[198] Password requirements must balance security with memorability. Clinic law firms may wish to provide additional guidance to ensure clinic personnel create secure passwords that are memorable (for example, by encouraging use of mnemonics).[199] Finally, clinic law firms should consider requiring students to create different passwords for each technology platform (email, case management system, cloud storage account, etc.) used for clinic work.[200]

---

192 *See* Lanterman, *supra* note 19, at 19. R

193 NAT'L INSTITUTE OF STANDARDS & TECHNOLOGY, U.S. DEP'T OF COMMERCE, DIGITAL IDENTITY GUIDELINES: AUTHENTICATION AND LIFECYCLE MANAGEMENT 67–69 (Jun. 2017), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf.

194 *Choosing and Protecting Passwords*, CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY, DEPARTMENT OF HOMELAND SECURITY, https://www.cisa.gov/uscert/ncas/tips/ST04-002 (last revised Nov. 18, 2019).

195 *Id.*

196 *But see* Shira Ovide, *Everything You've Been Told About Passwords Is a Lie*, WASHINGTON POST (Jan. 10, 2023), https://www.washingtonpost.com/technology/2023/01/10/lastpass-breach-kill-passwords/ ("To create the best password, try to make it at least 16 characters. The more characters, the more time hackers need to guess your password.").

197 *See Choosing and Protecting Passwords*, *supra* note 194 ("For example, "'attern2baseball#4mYmiemale!' would be a strong password because it has 28 characters and includes the upper and lowercase letters, numbers, and special characters."). R

198 *See* DIGITAL IDENTITY GUIDELINES, *supra* note 193, at 67. R

199 *Id.*

200 "Use the following techniques to develop unique passwords for each of your accounts:

- Use different passwords on different systems and accounts.

2. Smart Phones and Mobile Devices

Additional considerations arise for smart phones and other mobile devices. At present, most phone calls and text messages are not sufficiently encrypted, meaning that "governments or anyone else with power over the phone company [can] read [the] messages or record [the] calls."[201] Additionally, many email and cloud storage providers allow access through mobile applications, which creates an additional access point to client data. Finally, clinic personnel may use their mobile devices for other common lawyering tasks, like taking pictures for fact investigation, receiving recordings or files from a client through text message, and so on. These each risk prohibited access to client data, and in some cases store client data on the device itself. For those reasons, it is important that clinic law firms create clear guidance for clinic personnel on how and how not to use their mobile devices, particularly when communicating with clients.

Clinic law firms should, at a minimum, require clinic personnel to password-protect their mobile devices.[202] Clinic law firms should consider requiring additional safeguards, such as biometric access through fingerprint or face recognition, automatically locking devices after a certain number of failed attempts to enter a password, and GPS tracking to locate a lost device containing client data. Additionally, clinic law firms should consider requiring clinic personnel to communicate with clients through more secure applications that offer end-to-end encryption for calls and text messages, like Signal and WhatsApp,[203]

- Use the longest password or passphrase permissible by each password system.
- Develop mnemonics to remember complex passwords.
- Consider using a password manager program to keep track of your passwords. (See more information below.)
- Do not use passwords that are based on personal information that can be easily accessed or guessed.
- Do not use words that can be found in any dictionary of any language."

Choosing and Protecting Passwords, *supra* note 194. R

201 ELEC. FRONTIER FOUND., *Communicating with Others*, SURVEILLANCE SELF-DEFENSE, https://ssd.eff.org/module/communicating-others (Jun. 8, 2020).

202 *See* Steven M. Puiszis, *Can't Live with Them, Can't Live Without Them: Ethical and Risk Management Issues for Law Firms That Adopt a "BYOD" Approach to Mobile Technology*, 2015 J. PRO. LAW. 33, 69–73 (2015) (listing potential terms for a "bring your own device" policy, including password protecting mobile devices).

203 *See, e.g.*, SIGNAL, https://signal.org/ (last visited Jan. 28, 2023) ("State-of-the-art end-to-end encryption . . . keeps your conversations secure. We can't read your messages or listen to your calls, and no one else can either."); *About End to End Encryption*, WHATSAPP https://faq.whatsapp.com/820124435853543 (last visited Jan. 28, 2023) ("WhatsApp's end-to-end encryption is used when you chat with another person using WhatsApp Messenger. End-to-end encryption ensures only you and the person you're communicating with can read or listen to what is sent, and nobody in between, not even WhatsApp."). In many cases, however, applications like these require the recipient to install and use the application (as opposed to receiving the encrypted message as an SMS text message).

or iMessage.[204] Short of this, it may be sufficiently reasonable to permit clinic personnel to call clients through their personal phones, though communication with clients through text message should be limited to non-substantive communication (for example, scheduling) to protect client confidences. If clinic law firms permit clinic personnel to use text message to communicate confidential information with clients, it should be because no reasonable alternative exists, they have informed the client of the risks, and the totality of the circumstances render that use reasonable.

Clinic law firms should create directives about whether, and under what circumstances, mobile devices can be used to store client data (like pictures, video or audio recordings, and PDFs). If the clinic law firm permits clinic personnel to store client data on personal devices to any extent, the clinic law firm should create procedures for how clinic personnel will securely delete that data when they are no longer part of the clinic law firm. Finally, clinic law firms should require students to immediately report to clinic supervisors when their mobile device is lost or compromised.

C. Who Can (and Cannot) See Client Data? Access by Clinic Personnel, Law School Employees, and University Employees

Clinic law firms must identify which university and law school employees are part of the clinic law firm and, accordingly, regulate who in the university has access to client data. How clinics approach this issue depends on the structure of university and law school staff. Some law schools have IT departments of their own, which fully control law school technology systems. Others have separate IT staff, but rely on university IT to maintain the systems used by the law school.

Relatedly, clinics should identify other law school staff who may access client data by supporting clinic faculty. Many clinic law firms employ staff assistants who work exclusively on clinic client matters or to support clinical faculty, much like a staff assistant at a law firm.

---

[204] *Messages and Privacy*, APPLE, https://www.apple.com/legal/privacy/data/en/messages/ (last visited Jan. 29, 2023). iMessage does not require a separate application, but does require that both sender and recipient use an iPhone or other Apple device. However, unless the option is disabled, iMessage conversations may be stored directly to the sender's and the recipient's iCloud accounts, which presents all of the risks discussed above, *see supra* Section III.A.2, regarding cloud storage. *Access Your Messages on All Your Apple Devices*, APPLE, https://support.apple.com/guide/messages/access-messages-apple-devices-icht5b5d1e63/mac (last visited Jan. 29, 2023). As of the date of this writing, FaceTime calls and messages are also end-to-end encrypted. *FaceTime Security*, APPLE PLATFORM SECURITY https://support.apple.com/guide/security/facetime-security-seca331c55cd/web (last visited Jan. 28, 2023).

However, some law schools may assign staff assistants to support both clinical and non-clinical faculty, or may not specify which assistants support clinics and which do not. Whatever the organizational structure, the clinic law firm must identify and train employees who will act as nonlawyer assistants of the law firm, and take reasonable steps to prevent all other university and law school employees from accessing client data.

First, the clinic law firm should identify which staff should (or, under particular circumstances, must) have access to client data. Those employees should be treated like nonlawyer assistants of the firm.[205] For example, all employees who will access client data should sign confidentiality agreements obligating those employees not to misuse or risk the exposure of client data. Those employees should also receive reasonable training to ensure they understand how to protect client data and what is and is not appropriate.

Second, the clinic law firm should create written understandings or agreements with university and/or law school employees who could, but should not, access client data. For example, if a law school's IT staff are part of a wider university IT department and have access to the clinic law firm's cloud storage, the clinic law firm should document an understanding that university IT staff will not attempt to access clinic client data, and take steps to ensure those employees are informed and trained accordingly. In some cases, university personnel may be eager to ensure clinic client data is afforded sufficient protection to avoid liability.[206]

D. How Will Clinic Personnel Use Email?

Email presents a series of challenges for the clinic law firm. Initially, email presents challenges similar to cloud storage, in that all emails sent and received using cloud-based email providers are stored on remote servers. As a result, the protections afforded to clinic law firm email accounts matter a great deal. Some law schools provide clinic students with new, clinic-law-firm-specific email addresses. Others have law-school email addresses operated and maintained separately from the university. Still others have email addresses maintained in the same package as email addresses for other divisions of the university. Whatever the agreement, the email service used in the clinic law firm must be protected as reasonably as client data in cloud

[205] MODEL RULES OF PRO. CONDUCT r. 5.3 (AM. BAR ASS'N, 2020).

[206] Other clinic law firms may have a less productive relationship with university personnel and fear that pointing out these vulnerabilities could undermine the clinical program. Each clinic law firm should decide, given its own position, how to balance these factors and the choices made around technology to ensure reasonableness under the circumstances.

storage.[207]

Additionally, other university and law school employees may have access to student email accounts. For example, the university's general counsel may need to sort through emails if served with a subpoena for records. In searching for responsive emails, the general counsel would need to know to identify and segregate emails that are protected by the attorney-client privilege. If that arrangement were not in place, general counsel could release emails responsive to the subpoena that include client confidences, and therefore cause the clinic law firm and its attorneys to violate their ethical obligations by not taking reasonable steps to prevent the disclosure.

Next, clinic personnel should disable automatic email forwarding from their clinic or university email to any other personal email accounts. Automatic email forwarding is commonly used to consolidate multiple email accounts into one inbox.[208] However, once emails are sent to a personal account, they are stored on the new account's server. Even if the clinic law firm has taken steps to protect university email accounts, the student's personal account is likely not so protected, making that client data vulnerable.

Finally, emails are susceptible to hacking and other intrusion. To avoid those intrusions, most email providers allow for encrypting email. As a general matter, emails do not necessarily require encryption unless they contain information of a particularly sensitive nature,[209] assuming that the emails are sent through a "reputable Internet service provider."[210] However, if the email is potentially accessible to third parties, encryption may be required.[211]

To address these myriad challenges, clinics should take steps to maximize the protection afforded to clinic-related emails. Ideally, the clinic law firm will have its own domain name (the name that appears after the "@"), subject to its own contract with all the measures suggested above regarding cloud storage. *See* Appendix A. Alternatively, assuming the law school or university email accounts are protected by those guarantees, the clinic law firm could create a separate set of accounts through the law school or university domain name that differentiate them from other university emails (for example,

[207] *See supra* Section III.A.2.

[208] *See, e.g.*, *Automatically Forward Gmail Messages to Another Account*, GMAIL HELP, https://support.google.com/mail/answer/10957?hl=EN (last visited Jan. 28, 2023); *Add Another Email Account to the Gmail App*, GMAIL HELP, https://support.google.com/mail/answer/6078445 (last visited Jan. 28, 2023).

[209] *See* ABA Formal Op. 477, *supra* note 8. R

[210] *See* Sisk & Halbur, *supra* note 14, at 1286; *see also* ABA Comm. on Ethics & Pro. Resp., Formal Op. 413 (1999). R

[211] *See, e.g.*, Pro. Ethics Comm. for the State Bar of Tex., Op. 648 (2015).

"lawclinic.studentname@university.edu").

However, that may not be possible at all law schools. Some clinical programs may not have the funding to secure a separate domain name or accounts through an email service provider. Additionally, maintaining email servers requires IT staff that universities and law schools may not be able to provide. If it is not possible for the clinic law firm to obtain its own domain name or accounts, the clinic law firm should ensure that whatever agreement applies to clinic personnel's email accounts includes protections around client data. *See* Appendix A.

Additionally, clinic law firms should create and train clinic personnel[212] on an internal protocol around email use. The protocol should, at a minimum:

- Require clinic faculty, staff, and students to add automatically-generated standard language regarding unintentional disclosures to all emails and replies to emails, on all devices;
- Require clinic faculty, staff, and students to only use a designated email address for all client-related correspondence;
- Prohibit automatically forwarding emails from the designated email address to any other email accounts; and
- Consider encrypting emails that contain client data subject to heightened protections.[213]

Clinic law firms should create standard practices around preserving emails for the client file, to ensure communications and records are not lost if the student's university email account is closed, rendering the student's clinic-related correspondence unavailable.

Clinic law firms should consider, however, that encrypting emails also creates potential challenges for recipients. Encrypting emails on web-based email platforms typically requires that the receiving party use a specific application or process to log in and open the email.[214] Clients or other recipients who are not familiar with these processes may have difficulty opening encrypted emails, particularly on mobile devices. Clinic law firms should consider the benefits and risks of email encryption for the specific matter types and clients they serve, the specific requirements imposed by local laws[215] and ethics bod-

[212] *See* MODEL RULES OF PRO. CONDUCT rr. 5.1, 5.2, 5.3 (AM. BAR ASS'N, 2020).

[213] *See* ABA Formal Op. 477, *supra* note 8. R

[214] Joel Witts, *What Is Email Encryption, How Does It Work, and How Can It Protect Your Organization?*, EXPERT INSIGHTS (Sept. 22, 2022), https://expertinsights.com/insights/what-is-email-encryption-how-does-it-work-and-how-can-it-protect-your-organization/.

[215] *See supra* Section II.B.1; *see infra* note 221 and accompanying text. R

ies,[216] and whether clients can give informed consent to receive unencrypted emails.[217]

E. Electronic Document Transmission

Clinic law firms must take reasonable precautions to protect client metadata in electronic documents when they are transmitted electronically (through email or otherwise). Electronic documents contain both visible and invisible client data. For example, an electronic document relating to a client matter contains visible information about the client in the words it uses to communicate. The document also contains invisible data about the client called metadata, or "data about data,"[218] which can be used to "describe[ ] the history, tracking, or management of an electronic document."[219] Metadata can show prior versions of the document, text that was deleted or replaced, editing history, and other information that may be protected by the duty of confidentiality.

Clinic law firms should ensure that clinic personnel remove metadata from documents before sending them outside of the clinic law firm. Applications like Microsoft Word and Adobe Acrobat allow users to wipe metadata from a document fairly easily. Clinic law firms should include instructions for doing so in their technology use policy.[220]

Clinic law firms must also create protocols around the distribution of personally identifiable information (PII)—information like a person's Social Security number, state-issued ID number, driver's license number, or financial account number. Some jurisdictions have laws or regulations specifically requiring organizations handling PII to create written protocols to prevent identity theft.[221] Clinic law firms

---

[216] *See, e.g.*, Pro. Ethics Comm. for the State Bar of Tex., Op. 648 (2015); *see also supra* note 162. R

[217] *See infra* Section III.G.

[218] *See* Hricik, *supra* note 105, at 80 (quoting Gerald J. Hoenig, *Technology Property*, PROB. & PROP., Sept./Oct. 2004, at 51, 51). R

[219] Riccardo Tremolada, *The Legal Ethics of Metadata: Accidental Discovery of Inadvertently Sent Metadata and the Ethics of Taking Advantage of Others' Mistakes*, RICH. J.L. & TECH., no. 4, 2019, at 5 (internal quotation marks omitted).

[220] Additionally, "attorneys undoubtedly must stay current with technology, including . . . the transmission of electronic documents and metadata, and the associated risks. The responsibility . . . also includes becoming familiar with scrubbing software, how to use the software, and ensuring that colleagues and administrative assistants are educated about and are actually using the software." Elizabeth W. King, *The Ethics of Mining for Metadata Outside of Formal Discovery*, 113 PENN ST. L. REV. 801, 829 (2009); *see also id.* at 829 nn. 158–59 (citing state ethics opinions on protecting metadata).

[221] *See, e.g.*, M.G.L. c. 93H & 201 C.M.R. 17.00 *et seq*. (requiring any person or entity that "receives, stores, maintains, processes, or otherwise has access to" a Massachusetts resident's personal information, including Social Security number, driver's license number,

should consider requiring any documents that contain PII to be transmitted using a case management software's secure portal. If that service is not available, clinic law firms should, at a minimum, require the encryption of emails that contain PII or an attachment that includes PII.

F. Special Considerations for Public Law Schools Subject to Freedom of Information Laws

Clinic law firms at public universities must consider whether their jurisdiction's Freedom of Information Act or sunshine laws (hereinafter "FOIA laws")[222] might be used to seek, or could cause the inadvertent disclosure of, client data. FOIA laws permit members of the public to request access to public records.[223] FOIA laws typically define the term "public records" to include a broad swath of material.[224] Some public records, however, are exempt from disclosure.[225] When a member of the public requests records from a government entity, the entity must identify the material responsive to the request and then provide copies of the records or inform the requesting party of any materials withheld under an exemption.[226]

Because public law schools are treated as government entities,[227] their records are generally subject to state FOIA laws.[228] Law school clinics at public universities, as part of the law school, are also poten-

or financial account number, to create a "comprehensive information security program" to protect that information); *see also* ANDREW B. SERWIN, INFORMATION SECURITY AND PRIVACY: A GUIDE TO FEDERAL AND STATE LAW AND COMPLIANCE §§ 25:46 to 25:522, Westlaw (Nov. 2022 update) (providing a survey of state-specific laws regarding security breaches, including regulation of the storage and distribution of personally identifiable information).

222 For simplicity, I use the terms "FOIA laws" to refer to any state laws that allow the public to request public records, and "FOIA requests" to refer to requests made under such a law, even though some state laws have other names. *See, e.g.*, N.J. STAT. ANN. § 47:1A-1.1 ("Open Public Records Act").

223 For a list of each state's FOIA equivalent, see Elizabeth O'Connor Tomlinson, *Litigation Under Freedom of Information Act*, 110 AM. JUR. TRIALS 367, § 35, Westlaw (database updated Nov. 2022).

224 *See, e.g.*, D.C. CODE ANN. §§ 2-502(18), 2-539(a)(10); N.J. STAT. ANN. § 47:1A-1.1.

225 5 U.S.C. § 552(b).

226 *See, e.g.*, D.C. CODE ANN. § 2-532(c)(1) ("[A] public body, upon request reasonably describing any public record, shall within 15 days . . . of the receipt of any such request either make the requested public record accessible or notify the person making such request of its determination not to make the requested public record or any part thereof accessible and the reasons therefor."); *see also id.* at § 2-533(a) (denial letter must include reasons, including any exemptions claimed).

227 Nat'l Collegiate Athletic Ass'n v. Tarkanian, 488 U.S. 179, 192 (1988) ("[A] state university without question is a state actor.").

228 Lee R. Remington, *School Internet Investigations of Employees, Open Records Laws, and the Prying Press*, 31 J.L. & EDUC. 459, 460 (2002); *see also, e.g.*, Bauer v. Kincaid, 759 F. Supp. 575, 582–83 (W.D. Mo. 1991).

tially subject to those requests, subject to exemptions.[229] The New Jersey Supreme Court has explicitly addressed this question with respect to clinics at Rutgers Law School, concluding that "records related to cases at public law school clinics are not subject to [the New Jersey FOIA law]" at all and that the law therefore cannot be used to request "client-related documents," "clinical case files," or "information about the development and management of litigation."[230] Other jurisdictions have not squarely addressed the question and, therefore, clinic law firms should prepare to shield client data that might otherwise be released in response to FOIA requests.

To that end, it is important that clinic law firms at public universities address three related issues. First, clinic law firms must identify which university personnel are responsible for responding to FOIA requests, and create a system through which clinic client data can be segregated and exempted from disclosure. At some universities, university general counsel may respond to FOIA requests. Others may designate a specific office or administrative staff to do so. Identifying the responsible university personnel matters for two key reasons. Initially, allowing those personnel access to client data for review could breach the duty of confidentiality. As a result, those university personnel must either be treated as part of the clinic law firm or asked to sign confidentiality agreements that adequately protect the client's confidences.[231] Just as importantly, because they will be handling clinic client data, these university personnel must be adequately trained to identify and shield it from disclosure.[232]

Second, whichever university personnel are charged with responding, they must have a clear understanding of how to identify and segregate clinic client data. For example, if the clinic law firm uses university email, they might provide a list of email addresses of clinic personnel each semester to allow client-related emails to be identified and segregated. Similarly, if the clinic law firm uses university cloud storage to store client data or work product, the clinic law firm might share the names of clinic personnel so that their accounts can be flagged to prevent disclosure.

---

229 Note, Jennifer Dearborn, *Ready, Aim, Fire: Employing Open Records Acts as Another Weapon Against Public Law School Clinics*, 39 RUTGERS L. REC. 16, 22 (2012) ("Law school clinics within public law schools, therefore, should turn over any relevant information within reason, such as financial data."). *But see* Jon C. Dubin, *The Rutgers Cases and the State of the Law of State Law School Clinical Programs*, 65 RUTGERS L. REV. 817, 821 (2013) ("At a minimum, . . . public law school clinical personnel should never be deemed state agents or actors when lawyering for private clients.").

230 Sussex Commons Assocs. v. Rutgers, 46 A.3d 536, 547 (N.J. 2012).

231 MODEL RULES OF PRO. CONDUCT r. 1.6 (AM. BAR ASS'N, 2020).

232 *Id.* at r. 5.3.

Third, clinic law firms must ensure that the university personnel responding to FOIA requests articulate the correct exemptions under which that information falls. The clinic law firm may advocate for the university to take the position adopted by the New Jersey Supreme Court in the Rutgers litigation to assert that the clinic law firm is not subject to FOIA requests.[233] Additionally, in many FOIA laws, documents and information protected by the attorney-client privilege are exempt from disclosure.[234] Some jurisdictions also explicitly shield documents and information protected by the work-product doctrine.[235] Of course, some communications and documents that *are* treated as client confidences under the rules of professional conduct are *not* protected by the attorney-client privilege or work-product doctrine.[236] For example, an email to a third party (not the client) must still be kept confidential, even though it is protected by neither the attorney-client privilege nor the work product doctrine. Clinics may be able to prevent disclosure of those materials under exemptions protecting "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy."[237]

To ensure that these procedures and legal analyses are consistently applied, the clinic law firm may wish to document them in a memorandum of understanding or written protocol with the applicable offices in the university. Clinic law firms should also ensure that the university alert them when new employees are tasked with responding to FOIA requests, so that the clinic law firm can ensure those employees are trained to follow the memorandum or protocol and sign a confidentiality agreement.

---

233 *See* Dubin, *supra* note 229, at 842–46 (summarizing the legal framework used by the New Jersey Supreme Court to preclude application of New Jersey's FOIA law, the Open Public Records Act, to Rutgers University); *see also Sussex Commons Assocs.*, 46 A.3d at 543–47. R

234 *See, e.g.*, 5 U.S.C. § 552(b)(5); Elec. Frontier Found. v. U.S. Dep't of Just., 739 F.3d 1, 4 (D.C. Cir. 2014) ("Exemption 5 covers material that would be protected from disclosure in litigation under one of the recognized evidentiary or discovery privileges, such as the attorney-client privilege.").

235 D.C. CODE ANN. § 2-534(e). *But see* Dubin, *supra* note 229, at 836 n.96 (2013). R

236 MODEL RULES PRO. CONDUCT r. 1.6 cmt. 3 ("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.").

237 5 U.S.C. § 522(b)(6); *see also* D.C. v. Fraternal Ord. of Police, Metro. Police Dep't Lab. Comm., 75 A.3d 259, 264–66 (D.C. 2013) (interpreting analogous exemption of D.C. FOIA, D.C. Code § 2-534(a)(2)).

G. Alternatives: Informed Consent to Limit Professional Obligations in Retainer Agreements

Some clinic supervisors may not be able to effectuate these policies and protections easily or at all. Initially, universities, law schools, and clinical programs are each structured differently. It may take time to ascertain the terms of contracts with technology vendors, internal university practice and staffing, and the appropriate decision makers vested with the power to make changes. Even upon finding that information, some clinic supervisors may lack the status, funding, or bargaining power to bring about needed change.[238]

Generally, a lawyer and client may agree to modify or limit a "mutable" duty under the rules of professional conduct,[239] so long as "the client is adequately informed and consents[ ] and . . . the terms of the limitation [or modification] are reasonable in the circumstances."[240] The duty of confidentiality is one such mutable obligation.[241] It is not clear, however, whether a client could enter an unqualified and prospective general waiver of the security of their data.[242]

Clinic supervisors may decide to obtain a client's informed, written consent to certain technology use that may be reasonable under circumstances where more protective measures are not practicable or would pose significant disruptions to the representation.[243] Clinics that work with organizational clients may already include such language in their retainer agreements or memoranda of understanding, and may be accustomed to negotiating an organizational client's preferred security measures.[244] Clinics that represent individual clients

[238] *See* Berger, *supra* note 85, at 136 n.30 (describing the various statuses afforded to clinic supervisors and the extent of their role in faculty governance); *see also generally* Adamson et al., *supra* note 86. R R

[239] Charles Silver & Kent Syverud, *The Professional Responsibilities of Insurance Defense Lawyers*, 45 DUKE L.J. 255, 306 (1995) (explaining that a mutable duty "can be altered, amended, or waived with a client's informed consent").

[240] RESTATEMENT (THIRD) OF THE LAW GOVERNING LAWYERS § 19(1) (AM. L. INST. 2000).

[241] *See* Silver & Syverud, *supra* note 239, at 308 ("The duty of confidentiality is an example of a mutable duty.") R

[242] The comments to the rule on waiving future conflicts of interest, while in a different context, may inform the potential limits on a client's ability to prospectively waive the confidentiality of their data. *Cf.* MODEL RULES OF PRO. CONDUCT r. 1.7 cmt. 22 (AM. BAR ASS'N, 2020) (noting that a "general and open ended" waiver of future potential conflicts is ineffective "because it is not reasonably likely that the client will have understood the material risks involved").

[243] *See* Scott Rothenberg, *Maintaining Client Confidentiality in the Digital Era*, 27 APP. ADVOC. 720, 725 (2015) (recommending that lawyers "educate the[ir] client[s] as to the benefits of communication through social media messaging, text messages, e-mail, secured e-mail, fax, digital fax, et cetera., versus the potential security drawbacks of each").

[244] For example, clinics representing organizational clients might raise these issues when

should consider whether it is appropriate to counsel the client on any limitations or risks presented by a clinic law firm's technological capacity. Indeed, ABA Opinion 483 suggests that "[a]t the beginning of the client-lawyer relationship, the lawyer and client should discuss what levels of security will be necessary for each electronic communication about client matters."[245]

It is also important to note that the requirements of the rules of professional conduct do not always meet the realities of poverty lawyering.[246] Even when higher-security measures are available, they may be squarely incompatible with the communication needs of a client in crisis or one living in poverty. For example, while the reasonableness standard may suggest an email be encrypted, encryption may prevent a client from opening it due to additional steps needed to do so, like downloading a specific application. Similarly, if clinic personnel can only use their personal devices to send and receive text messages, the client's interests may be best served by mutual, informed consent to text messaging on those personal devices. The key to these agreements is to adequately inform the client of the risks and potential consequences of their choice, such that any limitations to which they agree are made with informed consent and are themselves reasonable under the circumstances.[247]

At the same time, clinic personnel should be careful to adequately explain the risks of insecure technology use to the client, and avoid glossing over or minimizing them. Disparities in bargaining power between lawyers and clients can lead to unintended pressure for a client to agree to the limits, especially if the lawyer will not represent them otherwise. Clinic personnel must be as specific as possible in identifying and explaining the particular risks posed by particular technology (or lack thereof), such that the client can anticipate the specific consequences they might face.[248] It is worth considering whether a client's consent to certain risks can ever be truly informed, particularly where the client's alternative is to forego legal representation.

---

forming representation agreements or memoranda of understanding, and include language in those agreements through which the client acknowledges the cloud storage platforms the clinic will use to store its data, and waives any claims related to that use.

[245] *See* ABA Formal Op. 477, *supra* note 8, at 7. R

[246] *See* Theresa Glennon, *Lawyers and Caring: Building an Ethic of Care into Professional Responsibility*, 43 HASTINGS L.J. 1175, 1178–85 (1992) (espousing an "ethic of care" in understanding and applying rules of professional conduct).

[247] *See* Rothenberg, *supra* note 243, at 725. R

[248] *Cf.* MODEL RULES OF PRO. CONDUCT r. 1.7 cmt. 22 (AM. BAR ASS'N, 2020) ("The more comprehensive the explanation of the types of future representations that might arise and the actual and reasonably foreseeable adverse consequences of those representations, the greater the likelihood that the client will have the requisite understanding.").

Additionally, this option should not be used as an "out" to avoid adherence to professional obligations for convenience. Instead, it should be considered as a last resort in the event decision makers outside the clinic law firm will not or cannot make some changes despite the clinic law firm's good faith efforts to secure them, or when modifying the obligation better serves the client.

Finally, clinic supervisors should ensure law students understand why and how these limitations are being negotiated. In particular, clinic supervisors may also wish to discuss the morality of asking clinic clients to contract away a professional duty.

CONCLUSION

When sharing this piece with colleagues, I noted a common reaction: fear; worry; panic. These colleagues expressed anxiety at the prospect that they were not competent in understanding clinic technology and its risks, that they did not know what if any protections were in place to shield their clients' data, and that the steps needed to address those issues were too daunting to contemplate. That reaction is understandable and important—yet it also offers another frame. This is an opportunity for clinical legal education to continue its tradition of moving to the forefront. Technology is a central part of law practice, and our students must be prepared to use it ethically. Shaping clinic law firm policies to comply with ethical rules also arms us to train our students to go into the legal community and ensure the same. Finally, it should compel the field of clinical legal education to establish systems for keeping up to date on an ever-changing technology landscape.

Technology is dynamic, and the guidelines offered in this piece cannot account for the specific ways in which it might change. Indeed, it is jarring to read articles from only two decades ago that discuss technology that has already been updated or left behind. For that reason, the guidance in this piece reflects the current tech landscape and options available to law school clinics to engage it. But it must grow and evolve with the technology—and so must we.[249]

[249] *See* Richard Zorza, *Re-Conceptualizing the Relationship Between Legal Ethics and Technological Innovation in Legal Practice: From Threat to Opportunity*, 67 FORDHAM L. REV. 2659, 2684 (1999) ("[N]ew rules should encourage flexibility by stating their principles as generally as possible to accommodate the rapidly developing state of the art.").

Appendix A - Addendum on Cloud Storage Data Security Provisions

The following addendum shall be incorporated into the Agreement between [Law School Name] ("Subscriber") and [Provider Name] ("Provider") regarding Subscriber's use of the [Provider Product Name] product and service ("Product").

1. Purpose. The purpose of this addendum is to document the understanding between Subscriber and Provider regarding Provider's handling of any data, information, or material Subscriber provides or submits through the Product ("Subscriber Data").

2. Subscriber Personnel. As used in this Addendum, "Subscriber Personnel" shall refer to [Contact Name and Title] of the [University Name] [Clinic Law Firm Name]. Subscriber personnel can be contacted by email at [email@address] or by telephone at [number]. Subscriber will promptly notify Provider in writing in the event the identity and/or contact information for Subscriber Personnel should change.

3. Information Security Certifications. Provider agrees to take reasonable measures to protect the security of Subscriber Data, including but not limited to the following:

> 3.1 At all times, Provider will take reasonable measures to employ information security best practices for storing and transmitting Subscriber Data and to prevent a reasonably foreseeable attempt to infiltrate Subscriber Data;
>
> 3.2 At all times, Provider will take reasonable measures to employ information security best practices regarding network security, including but not limited to the use of firewalls, penetration testing, and authentication protocols;
>
> 3.3 At all times, Provider will take reasonable measures to ensure its facilities maintain compliance with the assurances provided to Subscriber during procurement of the Product [if specific documents or correspondence details those assurances, they might be attached or incorporated by reference]; and
>
> 3.4 At all times, Provider will take reasonable measures to employ information security best practices to back up Subscriber Data such that, in the event Subscriber Data is lost, corrupted, or otherwise affected, Subscriber Data can be restored and recov-

ered by Subscriber.

4. Ownership and Use of Subscriber Data. Subscriber retains complete ownership of all Subscriber Data. Provider agrees that it has no ownership or security interest in Subscriber Data. Provider further agrees that Provider will not collect, mine, save, disclose, or otherwise use any Subscriber Data for any purpose unless otherwise authorized by the Agreement; provided however, that Provider may use Subscriber Data in conjunction with the Product's intended use and/or related services (as defined in [Provider's Terms of Service, if they are memorialized outside the contract, online or elsewhere]) to Subscriber.

5. Confidentiality of Subscriber Data and Third Party Access. Provider understands that Subscriber's attorney-employees will use Product to store information that is subject to various jurisdictions' attorney-client privileges and which said attorney-employees must protect under various jurisdictions' codes of professional responsibility. Accordingly, Provider agrees as follows:

> 5.1 Provider will not release any Subscriber Data in any form, in whole or in part, to any third party unless expressly authorized in writing by Subscriber Personnel or as required by law.
>
> 5.2 Provider shall take reasonable measures to ensure that no employee, representative, or agent has access to Subscriber Data unless expressly permitted by Subscriber Personnel in writing, or unless otherwise permitted by the Agreement. In the event any Provider employee, representative, or agent, or any other person or entity, obtains unauthorized access to Subscriber Data, Provider shall strive to promptly (within 48 hours) notify Subscriber Personnel of such unauthorized access, and will further cooperate with Subscriber Personnel in a reasonable manner to identify the cause of the unauthorized access and any Subscriber Data affected. Upon reasonable request, Provider will collaborate with Subscriber and provide Subscriber Personnel with available security logs, records, or other information needed to identify the cause of the breach and any and all Subscriber Data affected.
>
> 5.3 In the event of a failure of information security or privacy, a data breach, a natural disaster, or any other event that may cause damage to, loss of, or unauthorized access to Subscriber Data, Provider shall strive to promptly (within 48 hours) notify Subscriber Personnel of such an event. Provider will further cooper-

ate with Subscriber Personnel in a reasonable manner to identify the cause of the breach and any Subscriber Data affected. Upon reasonable request, Provider will collaborate with Subscriber and provide Subscriber Personnel with available security logs or data needed to identify the cause of the breach and any data affected.

5.4 Unless prohibited by law, Provider will notify Subscriber Personnel of any requests by any third parties that Provider produce Subscriber Data to any third party, whether the request is made by legal instrument, orally, in writing, or by any other medium. In the event of such a request, Provider shall strive to promptly (within 48 hours) notify Subscriber Personnel of the request and shall afford Subscriber a reasonable opportunity to respond to the request before Provider produces the requested information. If Subscriber Data is the subject of a valid subpoena, is compelled by court order, or is the subject of any other legal instrument, Provider shall afford Subscriber a reasonable opportunity to legally intervene to protect its Subscriber Data through available legal processes before disclosing any Subscriber Data, unless expressly authorized in writing by Subscriber Personnel or unless required by law.

6. Storage Within the United States. Provider will store Subscriber Data within the geographic borders of the United States. Before storing Subscriber Data outside of the United States, Provider will notify Subscriber Personnel and offer Subscriber an opportunity to ensure that the jurisdiction in which Subscriber Data will be stored has privacy laws, data security laws, and protections against unlawful search and seizure that are at least as rigorous as those of the United States. In any event, Provider shall not store Subscriber Data outside of the United States without Subscriber's express consent in writing.

7. Treatment of Data upon Termination or Cessation of Business. If Provider ceases its business operations for any reason, or if the Agreement between Provider and Subscriber is terminated, or if the Product otherwise has a break in continuity, Provider will provide Subscriber a period of ninety (90) days from the date of termination or cessation to retrieve all Subscriber Data. After Subscriber has retrieved all Subscriber Data, Provider agrees to delete all Subscriber Data and backups of Subscriber Data from all Provider servers, devices, and facilities, and further agrees not to retain any copies or other reproductions of Subscriber Data or backups of Subscriber Data, in whole or in part.

APPENDIX B—OUTLINE OF CLINIC TECHNOLOGY USE POLICY

Below is an outline of the topics that might be covered in a clinic data security policy, and sample language regarding those provisions. The exact structure of the policy will vary widely based on the platforms, devices, and means available to the clinic law firm. At times, I bracket and italicize optional or context-specific language or guidance.

***

CLINIC TECHNOLOGY USE POLICY

I. INTRODUCTION AND PURPOSE

Technology use has great benefits to law practice. With those benefits come risks that our clients' information could be accessed without their consent. As student attorneys, your conduct must comply with the obligations of the Rules of Professional Conduct. The rules of professional conduct require that we take particular care when using technology to advance client work. The rules require that competent attorneys must "keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology." *See* MODEL R. PROF. CONDUCT 1.1. [*Clinic law firms will likely cite their jurisdiction's specific rules of professional conduct, depending on the jurisdictions in which their clinic supervisors practice.*] The rules also require that we take reasonable measures to uphold the duty of confidentiality. *See* MODEL R. PROF. CONDUCT 1.6.

This policy creates rules and procedures that every member of the clinic must follow to uphold their obligations under the rules of professional conduct. [*As applicable:* Your compliance with this policy will be assessed by your clinic supervisors throughout your time in clinic. Repeated or intentional noncompliance with these procedures will negatively affect your final grade, as determined by your clinic supervisor, and may also constitute a violation of the Law School's Honor Code.]

Following these rules not only protects your clients from having their confidential information accessed, but also protects you and your supervisors from inadvertently violating the rules of professional conduct. These policies reflect the requirements of practicing law in the technological age. Your careful compliance with them will both set you up for a successful [semester/year] in clinic, and prepare you to enter the legal community ready to ethically practice law.

If you have any questions about these policies or what they require,

contact your clinic supervisor [*or other designated clinic personnel, such as a managing attorney, Dean of Experiential Learning, IT staff, etc.*]. If you believe you or one of your colleagues has violated this policy, immediately report to your clinic supervisor. We will work together to resolve the issue.

II. Technology Platforms and Student Accounts

1. The Clinical program uses [Case Management System, hereinafter "CMS"] to manage all client matters. Your clinic supervisor will share the specific protocols for using [CMS] to manage clinic matters.

2. The Clinical program uses [email provider] for all clinic-related email correspondence. You should not use any other email account for clinic-related correspondence.

3. [*If applicable*:] The Clinical program also uses [cloud-based collaborative tool] for work on client matters.

4. [*Identify any other technology platform used across clinics, including e-fax accounts, collaborative tools, etc.*]

5. You will receive login credentials for each of these accounts from [source] at the start of your time in clinic. [*If applicable*: You already have access to [*some platforms*] through the Law School.] When you set up your account, create a strong password for each. Your password for each account must be different, and it must use at least 10 characters, including at least one capital letter, lowercase letter, number, and special character. Your passwords must not contain complete words or phrases. Additionally, you should not use numbers or words directly associated with your information (for example, do not use your birthday, street address, phone number, family names, etc.).

6. [*If available*:] You should enable two-factor authentication for [specific accounts that offer it].

III. Using Personal Devices for Clinic Work

1. You will be permitted to use your personal devices (laptop, tablets, and smart phone) for clinic work *only if you comply with this policy*. If you are unable to comply with any of these policies with respect to a device, you may not use it for clinic work.

2. Create a strong password (*see above*) or personal identification

number (PIN) for your computer, your smart phone, and any other device you will use for clinic work. [*Clinic law firms may choose to require clinic personnel to use biometric access tools, where available.*]

3. You may not use a device for clinic work if any person other than you uses or has the password for the device.

4. Ensure that each device has updated anti-virus software and has installed the most recent system update. [*Clinic law firms may wish to research and require use of particular anti-virus, anti-malware, or anti-spyware software.*]

5. You may only do clinic work through a secure Wi-Fi connection. You may only use your home internet connection for clinic work if it is password-protected. You may *never* use public Wi-Fi to do clinic work [unless you have made access to the work platform through a VPN, as described in Item 8 below].

6. After using an internet browser for any clinic work (including on [CMS], Westlaw or Lexis, email, and [cloud-based collaborative tool]), close all tabs in that browser completely to ensure that you are logged out of each.

7. All client work must be stored on [CMS] [and [cloud storage provider, if applicable]]. [*If applicable:* You should create and edit client work directly within [CMS and/or cloud-based collaborative tool].]

8. [*Clinic law firms that utilize a VPN or VDI should detail the specific procedures used to install it and use it to do clinic work.*]

9. You may not store *any* client work on your personal devices. That means you may not save files to your desktop, hard drive, external hard drive, or other device. If you have no choice but to download a file directly to your personal device, you must transfer it to [CMS or authorized cloud-based collaborative tool] as soon as practicable, and immediately delete it from your device. [*Clinic law firms should detail any exceptions to this policy, depending on the structure and capabilities of their case management system and cloud storage services.*]

10. [*If clinic law firm permits storage of client work on personal devices, it should consider language like the following:* Before using your personal computer to store client work, you must encrypt

the hard drive on the device using File Vault (for Macs), BitLocker (for Windows devices), or another approved encryption application.]

11. In the event any client work was stored on your personal device during your time in clinic, you must take specific steps to ensure that it is securely removed from your device at the end of your time in clinic. First, delete all client-related files on your device, including in your downloads folder. Then, you must work with [IT point of contact] to use [authorized "file shredding" application] to prevent the files from being recovered. If you have questions about how the file-shredding application works, contact [clinic law firm point of contact].

12. [*If applicable:* On each of your personal devices, enable biometric access tools like fingerprint or face recognition. Enable GPS tracking on each device. If your device allows it, enable the setting that automatically locks the device after a set number of failed access attempts.]

13. If a personal device you use for client work is lost or compromised, inform your clinic supervisor immediately.

IV. Email

1. You must use [designated email account] for all clinic-related emails. You may not use any other email account, including your personal email addresses [*if applicable:* or University or Law School email addresses].

2. You may *not* use automatic email forwarding or inbox integration from your [designated email account] to any other email account. This ensures clinic-related emails stay on protected servers through the authorized email account. If you have already set up automatic forwarding or inbox integration with [designated email account], disable it immediately.

3. In your [designated email account] *on each device*, add the following as an automatic signature block on *all emails and replies to emails*:

   —
   Your Name
   [Jurisdiction-specific term for practicing law student]
   Your Clinic Name
   [Law School Name]

Phone Number
[Clinic Mailing Address]

NOTICE: This communication is confidential and may contain information that is privileged, personal and private, or attorney work product. This communication is intended only for the named recipients; it is not intended for public dissemination. If you have received this communication in error, please advise the sender by reply email and immediately delete the message and any attachments without viewing, copying, or disclosing the contents. Thank you for your cooperation. [*Clinic law firms may wish to adjust this based on any particularities in the applicable jurisdiction's ethics opinions regarding inadvertent disclosure.*]

4. [*Clinic law firms may wish to require email encryption, either for all client-related emails or for emails containing specific information justifying heightened protections. The procedures applicable to this requirement will vary depending on the email provider or application used for encryption.*]

5. "Phishing" is the practice of using deceptive emails to secure personal or confidential information from the recipient. Never click a link or reply to an email you do not recognize. Common signs of a phishing email include generic email addresses or unfamiliar domain names; emails that do not include specific signature blocks; emails that purport to be from popular corporations but misspell the corporate name; or emails that offer payment or other benefits by clicking an unfamiliar link. If you have any question about whether an email is legitimate, contact [point of contact for suspicious emails].

V. Document Transmission

1. Electronic documents relating to client work must be transmitted securely. Before sending any document as an attachment over email outside of your clinic, ensure you have erased all metadata from the draft, including document history, track changes, and comments, unless your clinic supervisor specifically authorizes you to do otherwise. [*Clinic law schools may wish to include step-by-step processes for eliminating metadata in Microsoft Word and Adobe Acrobat as follows*:

   a. In Microsoft Word, accept all track changes and stop tracking; delete (do not just resolve) all comments. To remove metadata, go to File > Info > Check for Issues next to Inspect

the Document and click "Inspect the Document." Check all of the boxes and click "Inspect." Click "remove" next to "Document Properties and Personal Information." Save the Word document with a name you choose for the recipient to see before closing.

b. In Adobe Acrobat, go to File > Properties and click "Additional Metadata" in the "Description" tab. Remove all metadata, then click "OK." Save the PDF before closing.

Note that these instructions may change over time or vary depending on the operating system.]

2. *Never* send emails or documents outside the clinic that contain a client's personally identifiable information (PII), including their Social Security number, driver's license or state identification card number, and financial account number. [*If applicable:* Documents containing PII should be shared using [CMS]'s secure document sharing portal.] Consult with your clinic supervisor before sending *any* emails or attachments that includes a client's PII outside of the clinic.

VI. Text Messages and Phone Calls

[*This section of the protocol will vary drastically depending on the individual choices in the clinic law firm regarding the reasonableness of personal cell phone numbers for client communications. The following is a suggested protocol that balances the various applicable considerations, and assumes that clinic supervisors first attempt to obtain informed consent to communication through personal smart phones, with a preference for using an end-to-end encrypted application. This section may also change if the CMS allows users to send and receive text messages.*]

1. Phone call and text messages made from your personal device are not encrypted, meaning the government and cellular service provider may be able to access those communications. Applications like Signal and WhatsApp allows users to make calls and text with "end-to-end encryption," meaning third parties cannot access the contents of those communications.

2. You may *not* use your personal phone to call or send text messages related to a clinic matter *unless* your clinic supervisor confirms that the client or other relevant individuals in that matter have given their written, informed consent, after being informed of those risks. If your client has consented to using SMS or

iMessage to communicate, disable automatic backups of your text messages to cloud-based servers (like iCloud). If your client has only agreed to communicate using an end-to-end encrypted application, you may *only* communicate with them on your personal smart phone using that application. Consult with your clinic supervisor to confirm what methods of communication are permissible in each of your clinic matters.

3. In clinic matters where the client or other relevant individuals have not consented to communicate through your personal devices, consult your clinic supervisor to create a plan for consistent client communication using email and clinic phones at the law school.

4. You should ensure that you log all client communications in [CMS] consistent with your individual clinic's policy. If you are unsure what communications to log or how to log them, consult your clinic supervisor.

5. At the end of your time in clinic, *after* you have logged all communications, you must delete all clinic-related conversations from your device (including, if relevant, the Signal or WhatsApp applications). Please note that when you delete a conversation, it is removed from your device and you cannot recover it.