APPENDIX 10

Clinical Programs
Policies Regarding Document Security and Use of Technology

As Student Attorneys enrolled in Suffolk University Clinical Programs, you will have access to a range of case-related information, confidential client data, and other confidential materials necessary for your work in Clinic. This access comes with significant responsibilities under federal and state laws, as well as under the ethical rules that govern legal practice in Massachusetts. In short, you are the custodians of the data and information you acquire, handle, and use on behalf of your clients. The guidelines below will be strictly enforced by your clinical supervisor. Adherence to these guidelines is an important aspect of professionalism, as well as your ethical responsibility to your clients. Your clinical grade will reflect your compliance with these procedures. These are our core policies governing the security of our legal practice and our clients' information, but they are not meant to be exhaustive or cover every situation. You will receive training on these protocols during orientation and feedback and mentoring on these and other security protocols throughout your time in Clinic. If you have questions at any time about these or other policies concerning the security of our legal practice and our clients' information, please speak with your supervisor.

If you believe there has been a security incident, or you or your colleague has violated these procedures, please immediately report the incident to your Clinical supervisor!

I. Email Accounts

1. You have been assigned a Clinical Programs "work email" – cl.student@suffolk.edu. This is the email you should utilize for all clinical case-related transmissions. You must never use your Suffolk University Office 365 email account or any other email account to conduct clinic-related business. Use only your assigned Clinical Programs email for all case-related business, whether those emails are directed internally (to your colleagues or supervisor) or externally (to opposing counsel, clients, etc.). You may use your Office 365 student email to communicate with your professors about class assignments or other non-case related business only. There are no exceptions to this rule.

2. You will receive a temporary password for your Clinical Programs email account. You will be prompted to update and change that password. You should create a unique and strong password for this account that is not one utilized for any other purpose. Strong passwords contain letters, numbers, and characters.

3. Never auto forward or forward your Clinical Programs emails to any other email account. Once you have done so, you expose that email and its contents to further distribution or hacking, and open up your personal email account to future discovery in litigation.

4. You may use your mobile phone to check your Clinical Programs email, but only if that device is pin or password protected and set to auto-lock. If you have set up

your Clinical Programs email on your mobile phone, you must delete that email account from your phone at the end of the school year. If you have opened or viewed on your mobile device any documents attached to emails, there may be remnants of those documents on your phone that must be removed at the end of the school year. If you have questions about how to remove these remnants, please visit the IT Help Desk.

II. Clio and Cloud Storage

5. Clinical Programs uses Clio for case management. All clinic-related work must be documented in Clio. If documents, notes, phone calls, contact information, calendar entries, etc., are not recorded in Clio, it is as if they don't exist. You will not be given credit for the work, and you will jeopardize your Clinic's ability to document the work done on the case and/or transfer that case to future Student Attorneys.

6. Clio is a Cloud-based program, meaning that it can be accessed online at www.goclio.com. That said, you may never access Clio without going through our secure virtual network (VDI). Prior to doing any work in Clio, you must be on a device that has installed the VDI. When using Clio through our VDI, all documents you view and/or download from Clio will be stored on Suffolk Clinical Programs secure drives. Those documents can then be uploaded by you back into Clio, where they will remain secure. At no time should you *ever* open, edit, or save – even temporarily – any case-related document on any computer or device without going through the VDI.

7. Never use OneDrive, Google Docs, Dropbox, or any other Cloud-based document sharing or document storage program for your clinical work. This is strictly prohibited and there are no exceptions to this rule.

III. Sending and Receiving Electronic Records

8. You must take special precautions when sending or receiving electronic records that may contain Personally Identifiable Information (PII) and other case-related information. PII is information that can be used on its own or in combination with other information to identify an individual, such as date of birth, name, financial account numbers, Social Security Number, address, license and ID numbers, etc. PII can be found in most pleadings, medical records, government records, bank records, discovery, etc. PII is subject to the requirements of M.G.L. c. 93H and 201 C.M.R. 17.00.

9. Never attach case-related documents that contain PII to emails unless those documents are encrypted. Documents may be encrypted using Clio's secure email function or using Suffolk University's email encryption system. You must obtain your supervisor's permission before attaching any case-related documents to an email using your Clinical Programs work email.

10. Never email any document outside of the clinic that contains track-changes, comments, or other editing notes, unless you specifically have your supervisor's authority to do so. Simply "hiding" tracked changes in Word (e.g. "Show Final Markup") *does not* get rid of the tracked changes. The person who receives the document can very easily change the view and see all of your edits. Always

"Accept All" changes in a Word document before sending it outside of Clinical Programs. As a general practice, you should convert Word documents into Pdf format before transmitting them electronically.

11. If you receive any document or electronically stored information relating to the representation of a clinic client that you believe was inadvertently sent to you by an outside party, please bring it to the attention of your supervisor. You may have an obligation to notify the sender. (*See* M.R.P.C. 4.4(b))

IV. Personal Computers and Mobile Devices

12. You may use a personal laptop or desktop to conduct Clinic work, provided you access all case-related information and material through the VDI – our remote, secured desktop. If you are not working in the VDI, you are not complying with this rule. Your Clinical supervisor reserves the right to check any and all personal devices for clinic materials at the end of the year. If clinic material is found on your personal devices, you will be required to work with IT to install scrubbing software and eliminate those files. Please note that other files and programs may be lost during the scrubbing process, so you should avoid working on personal computers and devices outside of the VDI.

13. Never use a public laptop or desktop to conduct any Clinic work.

14. You may not use any mobile device (phone, iPad, Kindle, etc.) to conduct Clinic work, with two exceptions. You may place cell phone calls, as needed and authorized by your Clinic Supervisors, and in compliance with the protocols set forth below. You may also use mobile devices to view and send clinic emails, provided you comply with the email protocols above.

15. You may *not* use the Clio Mobile App to view or access Clinic-related work. In an emergency situation when you need access to Clio (such as when in Court or off-site at a meeting), you may call Clinical Programs and ask a colleague or administrator to access the information from Clio on a clinical programs computer.

16. You may not use a personal cell phone to take photographs of case-related documents, evidence, or other case-related images unless you have your supervisor's permission and there is no alternative. Documents should be properly photocopied in the office. Evidence should be obtained using non-personal devices. If you must take photographs using your personal devices, you must disable Cloud-sharing and access to your photos by social media apps like Facebook, Instagram, Snapchat, etc. Clinic photos will need to be deleted from your phones at the earliest opportunity.

17. You may use the Clio Calendar to manage your clinic appointments and court dates. You may use the calendar on your mobile device or other electronic calendars to manage your time in Clinic, provided those entries do not contain any case information. For example, you may use case initials when entering a court date or meeting. Never enter case-related information in any personal, shared or public calendars.

18. Never place case-related documents on any personal USB device, thumb drives, or external hard drives. If you must use such a device, your supervisor can get you a

University-issued IronKey device that is encrypted and secured.

V. Meetings, Phone Calls, and Case Conversations

19. Case-related conversations and meetings, like phone calls, should be conducted in Clinical Programs spaces, out of earshot from individuals who are not associated with Clinical Programs. You may meet with clients and witnesses in Court and at their homes, or elsewhere, but only with your supervisor's permission.

20. When conducting case-related business on the telephone, be sure to make calls from a secure location so that members of the public and non-Clinic students cannot overhear. Avoid the temptation to take calls on the train, bus, or on the street. If you must do so, be discreet.

21. Never leave detailed voicemail messages containing confidential client information, unless specifically authorized to do so by the client and your supervisor.

22. At no time may you discuss or reveal *any information at all* related to any Clinical Programs case (yours or another student's) with *anyone* outside of your Clinic, unless authorized by your client for the purpose of representation and the conversation has been cleared in advance with your supervisor. It does not matter whether the information you wish to discuss is favorable to your client or already known in the litigation –the fact of representation itself is protected. It does not matter whether the case is closed or you are no longer enrolled in Clinic. Your duty to protect confidential case-related information is very broad and it lasts forever – even following the death of a client! There are very narrow exceptions to this rule that apply in very rare circumstances – and those situations should be discussed in advance with your supervisor. You must review and be very familiar with your obligations to protect client confidentiality under M.R.P.C. 1.6.

VI. Clinical Space, Paper Files and Case-Related Documents

23. All case-related documents must be maintained in the client file and kept in a secured clinical programs file cabinet when not in use. Do not keep loose papers associated with your case, as loose papers are easily lost and difficult to track. Do not keep files on desks, tables, near the copier or elsewhere when you are not using them. Never leave case-related files and documents in any public spaces.

24. You may not leave the Clinical Office with a client file or document without your supervisor's permission. You must maintain control over and protect the security of any and all case-related documents in your possession.

25. Avoid making excess duplicates of case-related documents. Make only those copies you will need.. You should shred (in the Clinical Programs shredders) excess duplicates.

26. You may only use Clinical printers to print, copy and scan case-related documents. You may not use the printers in the Suffolk University Law School library or any other non-clinical printers on campus for case-related information. You may not print from home printers without your Supervisor's express permission. Clio has been set up to print to the Clinical Programs printers. You may not use Clinical printers for any non-clinic related business.

27. The Clinical Program Suites (110, 140, 150, 160) are for clinical students, faculty, staff and clients only. You may not bring non-clinical friends or fellow students into the space. This ensures a safe, confidential environment in which you and your colleagues may perform legal work.

28. The doors on the Clinical Program Suites will be locked outside of business hours. You will receive a door code. You may not share this door code with anyone outside of Clinical Programs. You may not leave the door to any Clinical Programs suites propped open outside of business hours. This ensures the security of our client files and is meant to protect your safety.

THANK YOU FOR YOUR COOPERATION IN SECURING OUR LAW PRACTICE AND PROTECTING THE PRIVACY OF OUR CLIENTS!