

How to Protect Client Confidences in a Shared Office Space



Photo by
C & E

By Wells Anderson & Joseph M. Hartley



WELLS ANDERSON works with law firms throughout the country implementing practice management systems and offering technology advice.

E-mail: wa@wellslegaltech.com
Tel: 866-204-0007 612-791-0471
Web: <http://www.wellslegaltech.com>



JOE HARTLEY is a trial lawyer in Santa Monica, CA, where he advises lawyers and tries legal malpractice cases.

E-mail: jmh@hartley.com
Tel: 310.450.5316
Web: www.hartley.com

How to Protect Client Confidences in a Shared Office Space

Table of Contents

Introduction.....	3
Part I: Securing the Physical Layout.....	4
Chapter 1. How to Behave Around the Shared Office Suite	4
Chapter 2. Telephone Messages from Clients	6
Chapter 3. Faxes.....	7
Chapter 4. Incoming Mail.....	9
Chapter 5. Securing Confidential Information in Files.....	9
Chapter 6. Photocopying.....	10
Chapter 7. Securing Work Product	11
Chapter 8. Why You Need an Office Procedures Manual.....	12
Part II: Securing the Machines.....	13
Chapter 9. Securing the Single Computer.....	13
Chapter 10. Network Security.....	15
Chapter 11. Sharing Resources without Breaching Security	16
Chapter 13. Securing the Back-Ups.....	17
Chapter 14. Laptops.....	18
Chapter 15. Handheld Devices	18
Part III: Problems, Alternatives and the Future	19
Chapter 16. Potential Conflicts of Interest within the Shared Office Space.....	19
Chapter 17. Avoiding Ostensible Partnership.....	20
Chapter 18. Of Counsel vs. Sharing Office Space.....	21
Chapter 19. The future: Evaluating Emerging Technologies	22
Conclusion	23
Appendix.....	25
Appendix 1 Lawyer’s Shared Office Checklist	25
Appendix 2 Suggestions for Law Firms Renting Space to other lawyers	26
Bibliography	27

Copyright © 2002 Wells Anderson and Joseph M. Hartley - All rights reserved

Acknowledgements

The authors wish to thank Neil Squillante and Jennifer Katz of TechnoLawyer, www.technolawyer.com, for encouraging us to write this eBook and for their assistance in editing it. We also express our appreciation to the American Bar Association’s Law Practice Management Division and General Practice, Solo and Small Firm Section for publishing in *Law Practice Management* and *GPSOLO* our articles upon which this eBook is based. Special thanks go to American Executive Centers, www.aecphilly.com, 800-736-6034, for permission to use photographs from their attractive office suites in Pennsylvania and New Jersey.

How to Protect Client Confidences in a Shared Office Space

By Wells Anderson & Joseph M. Hartley

Difficult confidentiality issues arise from the very convenience of the shared office space. The key to avoiding breaches of confidentiality is to assume that every spoken word might be overheard and all written information might be seen. Then take appropriate precautions to protect your clients' confidences.

Introduction

The increasing expense of real estate as well as the amount of capital investment lawyers have to make in law office machinery and books make it quite expensive for solo and small firm lawyers to have the stand-alone, the well-appointed law offices most lawyers would like: an elegant reception area, quality art work on the walls, ample and spacious conference rooms, a full library, and offices with views. By combining several smaller firms or solo practices in a single location, many lawyers spread the high fixed costs of conference rooms, reception areas, library materials, photocopying, central phone system, fax, and other machines, making these amenities more affordable for all. The firms often have no business relationship among themselves; they simply share space together.

While the most common version of this cost-sharing arrangement is found in the shared suite, even large law firms are frequently subletting excess space to other lawyers and permitting use of the firm's physical facilities and equipment to subtenants. Besides the advantages of spreading the cost, being in the same space with other lawyers provides a built-in source of referrals. Economically, it is a good deal for all those involved.

A third variation is for law firms to share spaces with other businesses which are not law firms. It is not at all uncommon to find a group of like professionals—for example, lawyers and accountants—to share a common space. Sole practitioners with a major client often office in the same office suite as the client, even though the lawyer may have other clients as well.

Regardless of the form it takes, any shared-space arrangement raises serious questions of maintaining client confidences. Any person in the suite can gain access to confidential information if it is not protected. Any lawyer or law firm considering sharing space with other lawyers or law firms needs to consider carefully whether the layout of the shared office space will preserve confidentiality.

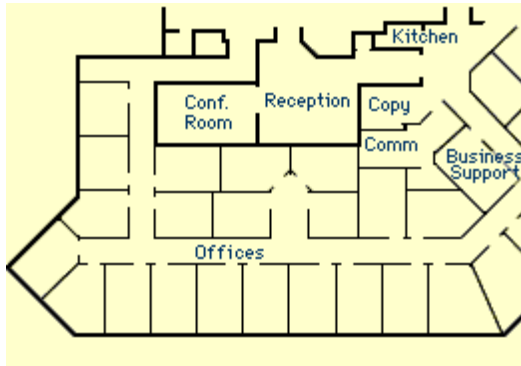
This e-book represents our experience in dealing with these difficult problems. Part I addresses the physical security of traditional client information such as conversations and paper. Part II addresses the changes that the personal computer has wrought and suggests

strategies to secure the firm's electronic data. Part III analyzes other implications of the shared office space, addresses alternatives, and gives some guidance for problems that might arise in the future through new technology and how, in any event, the lessons from the shared office space can be used by all lawyers in protecting client information as the legal world becomes more and more wired and dependent on networking devices.

Part I: Securing the Physical Layout

The shared office space is convenient and economical, but not secure. You cannot lock your secrets away behind close doors as you would if you had your own office.

Recognizing this feature is the key to protecting client confidences and avoiding conflict



Physical Layout
Image by AEC

of interest and malpractice problems. You need to be aware at all times that you are sharing space with other people. This part of the e-book examines the practical problems of law firms living together under a common roof. Chapters 1 through 4 discuss how to handle incoming communications from clients; Chapters 5 through 7 discuss the steps you need to protect sensitive information once it reaches your office. Chapter 8 shows why you need an office procedures manual to insure that you cover your bases in protecting client confidences in a shared office suite.

Chapter 1. How to Behave Around the Shared Office Suite

Before we even begin talking about how to protect different kinds of confidential client information that you are likely to find in the shared office suite, we need to discuss the



Talking in the
Halls
Photo by AEC

practicalities of being in a shared office suite. Simply put, you must assume at all times that persons other than in your firm will be able to see what anything that is written or overhear all conversations between you and your clients unless you take steps to ensure the confidentiality of the communication. Ask yourself a simple question: could anyone in this space overhear conversations between you and your client or get access to confidential written communications to or from the client? If the answer is "yes," then you are in a physical setting that will compromise the confidentiality of your communications. Asking and answering the question usually points the way toward how to protect the communications.

With that question in mind, the first step involved in recognizing the vulnerabilities in a shared office space is to recognize that you are not alone. Not only are other lawyers unconnected with your firm in the library, in the hallways, and

in the coffee room, but so may be their clients or other outsiders. To some extent, you are in hostile territory, and need to behave accordingly.

Here's a list of common problems we've seen with the way attorneys behave themselves in the shared office space:

Talking in the halls....or anywhere

Some lawyers like to start out talking to the client as soon as they see them in the reception area. This is poor form no matter where you are, but is disastrous in a shared office space. No talking with the client.

Conduct client conversations behind closed doors.

Many attorneys don't close the door when the client comes into the office. The client is thus seen by everyone who passes by in the hall, and can be heard by passers-by as well. We've even seen some attorneys interview clients in the library or other common areas when other people are passing through. All interviews with clients must be behind closed doors. No exceptions.

Tone down the phone conversation

Many attorneys have open-door policies, or feel claustrophobic if the door is closed. That's fine, but if you're talking to your clients, you better tone down the volume of your conversation. Even better, close the door (see above).

Don't leave confidential written material lying about

We'll discuss this topic in more detail later, but it is not uncommon for lawyers in shared office suites to take client files to the library or other common work areas. The file can sit there for days where the other lawyers, other clients, and the janitor can rifle through it. You simply cannot take confidential information outside your office.

Talking to the staff

Often attorneys will tell staff members to perform some task. The information conveyed to the staff member may be innocuous, or it may be highly confidential. To avoid having to make a determination of whether instructed a staff member in the hallway or coffee room might blow the attorney-client privilege, make it a practice to discuss assignments only in your office, preferably with the doors closed.

Be careful where you take your phone calls

If you're working in the library or in a common area where other suitemates have legitimate access, don't discuss anything confidential on your phone calls. Similarly, just because the lawyer from down the hall is shooting the breeze with you in your office doesn't mean he should hang around when you get a call from your client. If he does and you say something confidential to the client, you've probably waived the attorney-client privilege. You'd kick him out of the office if your client arrived; show the client the same courtesy when he phones.

This list is not intended to be exhaustive. Rather, its purpose is to get you thinking of possible breaches of confidentiality and how they might occur if you're not careful. With

this approach in mind, we'll now inventory the different ways that clients typically get information to their attorneys.

Chapter 2. Telephone Messages from Clients

We've already covered the situation where the client is talking to the attorney on the phone. But client may not reach the attorney directly and may have to leave a message. Each time the client leaves a message, there is a potentially for someone in the suite to see it. Here are the common situation and how to handle them.



Leaving Messages

Photo by AEC

Leaving messages with the receptionist

Many shared-space arrangements have a receptionist to field incoming calls for all the tenants. If the client leaves a substantive message with the receptionist, any attorney-client privilege is arguably waived. True, you could argue that the receptionist was reasonably necessary to get the message to you. But that's a difficult argument to make, complicated by agency questions (e.g., to whom does the receptionist owe a duty of loyalty?) And what if a confidential communication is written down on a pad for everyone to see?

The receptionist should be instructed to take no substantive messages from clients or, alternatively, to offer to transfer them to your voicemail. Similarly,

you should advise the client not even to attempt to leave confidential messages with the receptionist. The client will be pleased, not annoyed, that you're concerned about protecting confidentiality.

Leaving messages with other secretaries

Occasionally both the attorney and secretary are not available for a phone call, and another secretary in the office takes the call. As with the receptionist, the client must be instructed never leave any confidential message with anyone other than your voicemail or someone the client knows to be your employee.

Leaving messages with your secretary

Here, things get interesting. Under most state laws, a message to you through your secretary is just as protected as if it were made to you directly. The problems arise not in the fact of communication to you via your secretary, but in the manner in which the message is taken.

For example, a staff member speaking in a normal tone of voice can probably be heard by anyone passing by. If any confidential information is taken, the secretary must make it a practice (and you must make it a policy) to repeat the information only *sotto voce*. Staff members (and attorneys, for that matter) must make it a practice to know exactly where they are at all times and to assume that someone may be listening in. As in other areas of life, discretion is the better part of valor.

Answering machines

Many small firms have telephone answering machines on premises for after hours. The machines are fundamentally insecure; anyone can replay the message. Another problem is that they broadcast the caller's voice over a speaker while the caller is leaving a message. Most phone companies offer voicemail service that allows no one but you to access messages. It is certainly worth the additional cost to purchase voicemail service or equipment that secures access to messages through the use of a voice mailbox and password for each attorney.

Chapter 3. Faxes

We now move from oral communications with your clients to written communications. Occupying a middle ground between the two is the fax: a written communication that comes in by an analog phone. E-mail has not yet replaced the ancient and inefficient fax machines, so we can anticipate having faxes around for some time to come. The fax machine presents the most vexing problems of confidentiality in the shared office suite.



Protect Written Communications

Photo by AEC

Most shared office suites have a shared fax line. In fact, it is one of the conveniences a shared office suite usually offers as an incentive to its tenants. The new tenant does not have to install a separate phone line or bear the expense of maintaining it, and the communal fax machine is usually in a central, convenient area. And therein lies the problem.

If the client is sending you a confidential communication, a shared fax machine will not protect the confidentiality of your client's communication. If your opposition is sharp and realizes that you have a shared fax machine, you may be in for an unpleasant and expensive fight over the confidentiality of the faxes your client has sent you.

When fax machines first became available, they were much more expensive than they are today. Today a plain-paper fax machine with enough bells and whistles to satisfy even the most ardent gadget lover costs only a couple of hundred dollars. The fax/modem card (see below) is even cheaper and has also made secure receipt and sending possible from the computer. The rationale for sharing a fax is no longer economically compelling.

No confidentiality problems should exist when you send a fax if you or your secretary stand by the fax machine while it is sent. (You do need to have rules against leaving faxes unattended while they are being sent over a public fax machine.) Receiving faxes is different; no one from your firm is going to be standing over a shared fax monitoring what is coming through.

So, you need fax capabilities and you need confidentiality. Here are your options:

Fax card

Fax cards (fax/data modems) are now almost always included in new computers. As long as the computer with the fax card is using a line available only to your firm, and as long as the computer is either physically protected or otherwise made inaccessible by software protection as described later, confidentiality is protected.

On the downside, using a fax software is not so intuitive as using a fax machine. Some of the difficulties include negotiating menus for handling multiple attachments, adding scanned versions of paper documents to a fax, verifying that a fax has been sent successfully, and noticing when a new incoming fax has arrived. You and your staff can learn all these functions, but still it is easier to make errors with fax software than with regular fax machines.

Fax cards offer some advantages. Faxing straight out of a personal computer skips the manual paper handling involved in printing a feeding a regular fax. Sending to a group of people is easy rather than tedious like it is on a fax machine. The quality of the document seen by the recipient will be better since the fax software creates a more precise image of a word processing document. But some fax software may subtly alter margin sizes and even cause problems with page breaks.

If you are networked, you can receive and keep all faxes received through a fax card on a single machine, thus keeping copies of them for all posterity, as well as not wasting paper and toner on junk faxes. In addition, your faxes will be backed up onto the same tapes or other backup media that secure the rest of your computer records and documents.

If have a PC modem with fax capabilities connected to a phone line for other purposes, you may find sending faxes from your computer is convenient. But because of drawbacks for receiving faxes, you may want to use a stand-alone, plain paper fax machine for receiving faxes.

Personal fax machine

As an alternative to a shared fax machine or a fax card on your computer, you can have your own fax machine on a dedicated line without great expense. The main question here is where to put it. In our view, having a fax on a staff member's desk in open view is not much of an improvement on the common fax. The client's confidential communications are still open to everyone who passes by. Another option is to place it in one of the attorney's offices, with a firm rule that the door be closed and locked while the attorney is away. Many attorneys find the fax loud and annoying, although the ringer can be turned off.

Fax by e-mail

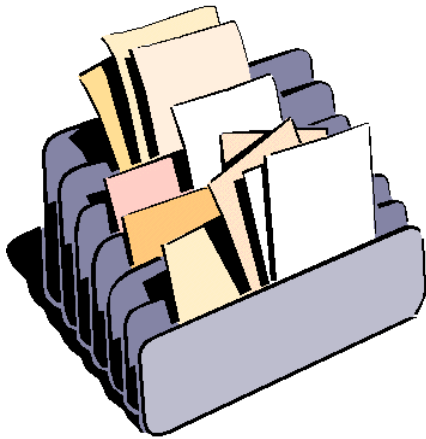
Some companies—MaxEmail, eFax and J2 come to mind—offer unique fax numbers for your private use. They forward faxes to your e-mail in-box as attachments to e-mail messages. You view the faxes through a free viewer the companies provide. As long as your computer and e-mail service are secure, these services can offer flexible alternatives to the traditional fax machine. They also permit you to get your faxes if you travel, an added bonus. You can even get a toll-free fax number, although at greater expense.

The services also offer the ability to fax from your computer so that you truly do not need

a fax line. The disadvantage of this option is that you either have to scan the documents you are sending or have a scanned letterhead and signature block (or signature fonts) to take full advantage of this option. The option of sending through a service is also expensive, although for someone who sends only a few faxes per month, the expense may be less than maintaining a separate fax line or paying to access the communal lines. As with most technology, your mileage may vary.

Chapter 4. Incoming Mail

The final way the firm in a shared office space is likely to receive information from its clients is by mail. Mail, by and large, presents fewer problems, provided that the firm keeps in mind that it is sharing office space with other lawyers.



Protect Incoming Mail

Photo by rogersgifs.com

Some shared-office arrangements have one person open and sort the mail for everyone in the office. This is an unbelievably bad idea that will cause real trouble sooner or later. Client mail must be delivered unopened to your office. No exceptions. If a receptionist opens the mail, you have just blown the attorney-client privilege for any privileged information. This also applies to any hand delivered documents from your clients.

Once you receive your mail, you cannot simply leave it lying around in an in-box for anyone in the suite to read. It must be opened and secured. Similarly, you cannot leave mail to a client in an outbox unless that box is secured. These problems are discussed in

greater detail in the Chapter 7, since their solution is identical to the problem of securing work product in general.

Chapter 5. Securing Confidential Information in Files

In the stand-alone firm, file storage does not present a problem of preserving confidences since files are usually stored in an areas of the firm away from the public where only members of the firm are permitted access. Many firms in shared office suites have opted for the convenience of centralized file storage that is shared with other suite members. Your files may be on separate shelves, but anyone in the suite has access to the file room and therefore access to your files. You, of course, have access to the other firms' files as well.

The major reason for centralized file storage is the convenience of knowing that the files are all in one place. To preserve the confidentiality, you have to make sure that no confidential documents are publicly available to members of the office suite. You have two choices. If you want the convenience and economy of using a central storage area, make sure that you store nothing confidential there. For transactional lawyers, this probably means that most files will have to be kept elsewhere. For litigators,

it means that you can keep all documents except privileged documents in the storage area. As a practical matter, that means that you keep your correspondence and memo file elsewhere, and keep pleadings, discovery, non-privileged documents, and the like in the shared file area. It is not as convenient as before, but you avoid no end of troubles.

The other option is having secure storage areas for all your files. Before you write this off as hopelessly unworkable overkill, consider that files need not be locked up during the day if some member of the firm is close by to control access. This approach can be as simple as a locked file cabinet at each secretary's workstation, or as complex as a locked office. Some attorneys don't mind having file storage in their offices which they lock each night. (Many do, however, since the support staff is usually running in and out to file or retrieve documents.) Either solution means you have to have more square footage to accommodate your files. In a firm of several lawyers, it also means that it may be harder for someone to find a given file since it could be stored in several locations.

Whichever solution you follow, you must implement proper security to insure that the files are protected. At a minimum this means a locked file cabinet. It means that the files should be locked up at the end of the day or if the staff member is going to lunch or will be out of the office for an extended period of time.

Chapter 6. Photocopying

Anyone looking at legal files generated in the 1940's or 1950's is struck at how much bigger files are today. We think this is in large part to the advent of the (relatively) cheap photocopying machine which allows all sorts of things to be copied and placed in the files, whether they are necessary or not.

And the shared photocopier is one of the real draws to a shared office space. Photocopier are still relatively expensive to own, and quite expensive to operate and maintain. Spreading the cost around a group of different lawyers can dramatically lower these costs.

The convenience of the photocopier comes with a price, though: the photocopier is available to everyone in the suite. That means that anyone making a photocopy cannot simply place the document to be copied in the feeder and walk away. The firm must have a rule that whoever is doing the photocopying never leaves the photocopy machine without removing the original and all copies.

Why must the firm have this rule? For the same reason that you should not attempt to store correspondence apart from the rest of the file: it requires both lawyers and staff to spend too much time thinking about whether a document is confidential or not. A simple rule avoids this problem, and assumes that everything being copied is confidential and therefore cannot be left in the photocopier while the photocopies are being made. Besides, it is annoying when another tenant in the suite comes in to make a photocopy and finds the previous batch from another office still in the machine.

We have written this chapter with the stand-alone photocopier as the model of how copies are made. However, the analysis would apply equally to any other method of copying used in the office. It is not unimaginable, for example, that shared office suites in the future may offer capacities to scan and organize written documents in digital form. In

such cases, the careful lawyer needs to be aware of both the security problems while performing the scanning (akin to photocopying) and the problems of using a communal or networked computer, which is discussed in Chapter 10. Technology will change, but the problems of confidentiality will not, and lawyers need to be aware of the impact that emerging technology will have on that problem.

Chapter 7. Securing Work Product

Protecting files means protecting final work product or correspondence. In the shared-space arrangement, thought must also be devoted to protecting such communications before they enter the filing system as well. In almost every firm that shares space with other lawyers, the secretarial cubicle is effectively a public area. Any tenant of the suite can gain access to it as easily as walking into a conference room or library. This feature is important both here and in the next section where we discuss computer security.

The fact that a secretarial cubicle is really a public space dictates the precautions that must be taken in a shared suite:

Work flow. If the secretary is working with a confidential document, that document must remain in sight of the secretary (and out of sight of any passersby) at all times. If the secretary leaves the area, the confidential document should be placed in a drawer.



In-box on Lawyer's Desk

Photo by AEC

Unread mail. Many lawyers like to have their in-box on their secretary's desk. In a shared suite, the secretary's desk sits in the public arena, and therefore is a lousy place for an in box. Better in the attorney's office.

Unedited work. Many secretaries place their work product into an in-box. For the same reasons as just discussed, the box is better

placed in the attorney's office. Alternatively, a drawer or other closed container at the secretary's desk could serve the purpose, though this arrangement raises the "out of sight, out of mind" problem that often results in misplaced or lost documents.

Filing. Most secretaries justifiably hate filing. In a stand-alone office, it doesn't really matter if the filing is done immediately or once a week in terms of protecting client confidences. In the shared-office space, it is critical that the filing be done immediately and the files returned to a secure location. If filing cannot be finished that day, it should be locked away when the secretary leaves for the day and finished the next morning.

Shared Printers. Since the price of a good, high-speed network printer has plummeted to around \$1300, sharing one with another firm in the suite no longer saves much money. The best approach is for each firm to have its own printers within easy reach and under the watchful eyes of its own staff. Just as you cannot leave a confidential document in a photocopier, neither can you print a confidential document to a remote printer unless someone from the firm is standing right there. All you need to do is make sure that the printer is either in a physically secure area or reachable by you within seconds after

hitting the print key. And, of course, you *must* go get the confidential document immediately.

Chron files. A chron file contains copies of everything the attorney has sent out, including confidential communications. Where is the chron file kept? In the secretaries unlocked desk? Not if you value your confidentiality. Lock it up with the other confidential information. Document management software offers an alternative to the chron file, providing the capability of listing the attorney's documents in date order with originals just a double-click away. Such software eliminates the busywork of maintaining an additional paper file of all work product.

Phone messages and message pads. Clients sometimes leave confidential communications telephone messages if their attorney is not available. Message slips should be guarded just like any other confidential communication. Message pads should be kept in a closed drawer after hours. We often recommend that the message pad be replaced with the electronic messaging available on most networked computers, provided that the network is secured. Case and matter management software now incorporates internal phone message features that can pop up small windows on attorneys' screens to notify them about important messages. In addition, these features automatically store phone messages, cross-indexing them by matter and attorney.

Note that the procedures recommended here do not distinguish between confidential information and information which is public. That's because there's entirely too much going on in a law office to permit two separate policies based on a staff member's determination that a particular document might be confidential. Not only would such a policy be entirely too cumbersome to enforce, it invites error by placing the responsibility for determining confidentiality on someone who is not an attorney. The simpler rule is to treat everything as though it is confidential, and avoid the problem in the first place. Besides, do you really want an office procedures manual that reads like the Internal Revenue Code?

One last item is the use—or rather, disposal—of drafts of confidential information. Some lawyers will keep the draft in the file forever. If you don't, you and your secretary need to take appropriate precautions to make sure the draft is unreadable by anyone who goes through your trash. Shredders are getting much cheaper, and are a sensible and inexpensive investment.

Chapter 8. Why You Need an Office Procedures Manual

Small offices generally do not have office procedures manuals. They take a lot of time and effort to prepare and often require negotiation of the details between the partners of the firm. Sole practitioners rarely see the need to document the fairly simple procedures of the firm in writing, even though the procedures can be quite complex.

Yet every lawyer or law firm in a shared office space needs an office procedures manual, if for no other reason that to remind both lawyers and staff about the need to protect client confidences. We've already covered seven major areas that lawyers sharing office space with others often do not consider. It is not reasonable to expect staff members to make the considerations when lawyers don't. Furthermore, if you get a new employee or

temporary employee in to replace a staff member who has left your employment, is ill or is on vacation, you need to be able to indoctrinate them fully and quickly. Do it in writing by a procedures manual, and you can insure you will cover everything.

The most important result of an office procedures manual, even for a sole practitioner, is that it forces the lawyer to think carefully about all the issues and dangers of the shared office space. Errors and omissions carriers often require such manuals. Even if they do not, simply sitting down and working through all the problems discussed in this e-book will be a significant step toward avoiding potential exposure and embarrassment to your clients.

Part II: Securing the Machines

Until the late 1970's, there would be no more to say about the pitfalls of sharing office space. The personal computer revolution, however, has had a profound impact on the problems of confidentiality facing a lawyer or firm that shares office space with others. Confidential documents now exist in electronic form, but many lawyers do not think about the steps necessary to insure the confidentiality of the machines. But electronic data is commonly considered to be a writing (see, e.g., Fed. Rule. Ev., Rule 1001(1)), and the lawyer who fails to protect this new form of writing faces needless exposure to malpractice and ethics claims. This part discusses the current technologies for securing your computers and other electronic devices, both at and away from the office.

Chapter 9. Securing the Single Computer

We start with the case of a single computer sitting on the desktop of the firm's secretary. On the computer's hard disk we find files for all the matters the firm is handling, including confidential communications to clients. Much of it is work product. The computer's hard disk may also contain the firm's billing and expense records and financial statements. You really don't want this information to be available. Yet there it is, sitting there on the desk, just waiting for anyone to sit down at the computer and take a look at what you have.



Securing Computers
Photo by AEC

Locking Up the PC

Some form of protection for the computer is required. The safest way to protect against unauthorized access is to lock the computer away. If the secretarial bay had a small, locked closet, for example, that would be the logical place for box containing the CPU and hard drive. No one but the firm could get access to it. As an additional benefit, a burglar inclined to carry off expensive electronic equipment would probably not want to waste time to break into a locked door when easier targets are available. Such an arrangement rarely exists in a shared-space arrangement, so other means must be found to secure the information on the computer.

Password Protection and encryption

The real defense you have is password protection and encryption. The idea is simple: you need a password to be able to get into the computer. Your computer will come with a BIOS password option, meaning that the computer will not even boot unless the word is typed in. A dedicated intruder intent on getting into your machine can pull the CMOS battery to disable the BIOS password, but that requires opening the computer case. You can purchase a case lock if the computer does not have one. Make sure your staff regularly turns off a computer protected in this fashion. As a first line of defense, it is good and the price (free with your machine) is right.

Caution: Do not assume that the “password” protection you get with Windows 95 or 98 is effective. By hitting the “escape” key, an intruder will still have access to all your files unless you’re able to set your machine up better than most.

The second defense is purchase security software to encrypt the entire hard drive or certain directories. These software products have become sophisticated in the way they encrypt the contents of a hard drive.

Protecting Passwords

Whatever you do, you will have to learn something about the proper use of passwords. Most passwords are easily discovered. People are so terrified that they will forget the password that they write down the password and tape it in an easily accessible “hidden” location. If you are going to undertake password protection, treat it seriously and devise a procedure that will give you some measure of security instead of the illusion of protection.



Protecting Passwords
Photo by openphoto.net

An underlying problem with passwords is that we each tend to accumulate too many of them: PIN numbers for cash machines, four digits to access voicemail, lock combinations, E-mail and Web services passwords – we can't keep them all in our heads. You can deal with the problem by encouraging your staff to write down their passwords, but hide them well. You can even help them find good places since they don't need to keep their passwords secret from you. You need to have the passwords of your staff to deal with situations such as vacations, turnover and disabilities.

Another basic problem with passwords is that people lose them. Anticipate this problem and be prepared to deal with it. Loss of a password to a single computer can be more devastating than loss of a network password, since you may have no other way into the computer. When selecting a computer encryption product, consider purchasing one that features both a user password and an administrator password. Then you will have a way to access the computer even if the primary user loses a password.

DriveCrypt has all the essential features you need, including user and master passwords, strong encryption, passive protection (the user does not have to remember to use it), and a reasonable price, \$39.95 per machine. It also supports a variety of advanced techniques

such as electronic USB keys and fingerprint readers. It is available via electronic download from: <http://www.drivecrypt.com>.

For additional information on electronic protection for your information, see the one-page article, *Be Safe! Privacy Tools*, in the March 2002 issue of Law Practice Management published by the American Bar Association. It is available on the Web at: www.abanet.org/lpm/magarticle2002_v28n2_p30.shtml

Chapter 10. Network Security

Increasingly sole practitioners and small firms are networking their computers, even in shared office spaces. It really isn't that difficult to do, since cabling usually can be snaked through existing walls and over the ceiling tiles to connect all computers.

There are three possible network configurations in the shared-space office:

1. A office-wide network connecting all computers and all members of the suite;
2. A peer-to-peer network with decentralized file storage connecting only the computers used by the firm but not by other suitemates; and
3. A file server network used only by the firm but where all the files are located on a single computer (the file server).

The first configuration is unacceptable unless very special precautions are used. Either of the other two methods of networks is acceptable but also requires appropriate precautions.

1. The office-wide network with one file server

Some offices are already wired for an office-wide network. All that the sole practitioner or small firm needs to do is install a network card and plug their PC into the network, giving it access to CD-ROMs, network printers, and even faxes. While this arrangement can offer convenience and savings to a small firm, it requires a network operating system expert to set up security features that will preserve client confidences.

Unless the network security is very carefully configured, you will have all of the problems that an unprotected, stand-alone system would have. Indeed, it is even worse, since only someone sitting at the computer can access the stand-alone system, whereas anyone on a network may be able to access the confidential files on your machine from their computer.

Benefits that this configuration gives are: (1) someone else serves as your network administrator (administering a network is complicated and time-consuming and therefore expensive), (2) it may give you access to a library of CD-ROMs or other purchased materials in electronic form, and (3) it allows for the easy sharing and exchange of other non-confidential materials through the use of "public" file folders. In this configuration, no member of a firm may have full access to the shared file server, so the firms must rely on an outside network company for support. It is good to have the file server in the care of experts, but the firms should have a clear understanding about guaranteed response time for service. When a single point of failure can stop multiple firms in their tracks,

they sorely need immediate help. Some companies can provide immediate assistance through a dial-up connection to the server, but this too must be highly secure.

When your vital work-in-progress is stored on a network file server, you can purchase software that serves as a safety net. Say you are putting the finishing touches on an agreement needed at a client meeting in one hour. The file server crashes. With document management software like Worldox installed, you don't have to worry. Worldox maintains mirrored copies of all your current documents on the C: drive of your computer. While the network is down, you can work with these copies as if they were the originals. This safety net is reassuring, but you will still want fast service for your network.

2. Separate peer-to-peer networks

An alternative network layout connects the computers of the firms in physically separate, peer-to-peer networks, one network per firm. In these networks, there is no centralized server. Each of the computers is separate and equal. Depending on how the topology is structured, it is possible to access files on various machines and preclude access on others. Access rights can be given to some files on a machine and not to others. So in a firm with associates, the partners could shield associates from reviewing the billing or accounting records.

The problems with this setup are identical to the stand-alone machines. In fact, they may be worse, since a computer in a public area may be able to access any other machine that is turned on.

3. Separate file server networks

Under this network arrangement, all of the data files for a single firm are kept on a single machine, the file server. Each person in the firm can access the file server using a username and password. Once again, the server should be locked away so that no one can access it directly. A server that can be accessed directly has the same problems as a stand-alone machine in a public area of the law firm.

The best solution to the networking problem is adequate password protection combined with physical security for the server. Ideally, the server would sit in a small room—preferably the size of a large walk-in closet—which would remain locked at all times and whose keys are carried by the members of the firm. (Leaving a key around is more convenient but defeats the security measures). With such security, the server can be kept running at all times without concern that unauthorized personnel could gain access to it. A suite containing a small storeroom or lockable, ventilated cabinet for the server would therefore be a decided plus for the small firm practitioner.

Chapter 11. Sharing Resources without Breaching Security

As the prices of devices such as fax machines, high quality color printers and scanners have plummeted, the financial advantages of sharing dropped with them. More and more services are available directly from the Internet. Since faster Internet connections have dropped in price too, subscriptions to legal research services and other resource have become much more affordable. Now it makes good sense to share a fast Internet

connection, but not printers and fax machines that produce confidential client documents you do not want to share.



Magnia SG20

Network Server
By Time Matters & Toshiba

The same argument applies to network servers. Once these computers commanded five-figure prices, but now all-in-one servers for staffs of about eight people can be purchased fully loaded and ready to use for under \$2,000.00. An example is the Toshiba Magnia SG20. This server allows multiple users to share files, printers, and an Internet connection. It includes dual hard drives, a network switch, a network operating system and software for E-mail, a firewall, and Web sites. For law firms, accountants and businesses that need to manage information on clients, cases, projects, tasks, schedules and documents, a version is available that includes practice management software from Time Matters preinstalled. See:

<http://www.timematters.com/products/linux/toshiba/index.asp> The low price for packages like this one make it far less compelling for multiple firms to use the same network and same server in order to save on hardware and setup services.

As a good rule of thumb, share information sources, such as an Internet connection and library, but not storage devices or output devices, such as a server and printer.

Chapter 12. Securing the Back-Ups

While a full discussion of backing up vital information could fill another book, security precautions deserve mention here. It is important that firms follow the first rule of back-ups: Store a daily back-up off-site. It is also important to protect the back-up against the possibility that it might fall into the wrong hands.

Most back-up software allows information to be encrypted with a password. We recommend using this feature. If the daily backup is stored off-site on tape, CD, hard disk or an Internet service, it is possible through accidental loss for the information to become available to a stranger. By protecting it with a password, you can make it impossible or at least impractical for anyone to access the backed-up information.

If you use passwords for back-ups, you run some additional risks. The password or the back-up software that can unencrypt the information could be lost. Be sure that more than one person has the password and that a copy of the software is stored off-site with the back-ups.

Internet services offer a very reliable approach to backing up information. A number of lawyers do not feel secure using a service that houses their confidential information “on the Internet.” Whenever you rely on a third party to protect your clients’ confidences, you face some additional risk. However, the risk of losing important information or disrupting your practice while you recover from a computer disaster is much more common. An established service provider with strong data encryption, such as Connected Corporation (<http://www.connected.com>), offers encrypted daily back-up that is more regular and reliable than tape back-up units.

Chapter 13. Laptops

Laptops have become much more common as prices have dropped. They can be connected at long distances with the office computer or network through a modem. This raises two potential attack threats, one at the level of the file server and the other at the location where the lawyer is trying to connect to his office.

On the file server, a modem means that the remote lawyer has an opportunity to dial in and get information. However, so does anyone else with a modem. While it is unlikely that the number would be discovered if the law firm does not publicize the number on which the modem is located, hackers call numbers at random looking for an open modem. Once a modem is discovered, they will try any series of passwords to try to gain access. These hackers use programs that make dictionary attacks as well as number attacks that try hundreds of possible passwords.

The second attack threat is with the mobile computer itself. A stand-alone desktop or tower computer at home will be sitting where it is under lock and key. Such machines rarely present a problem, but laptops present all the problems of a stand-alone machine in a public area of shared office space, and then some.

Laptops not only are easily accessible, but also can be stolen simply by unplugging and walking off with them. Many attorneys travel with a number of confidential files on their laptops, having copied or mirrored a directory from a file server so that the attorney can have full access to all materials that the law firm has.

Lawyers may use laptops in hostile territory, for example when depositions are taken in the office of the adversary's counsel. Rather than leaving a laptop unattended at a deposition, a lawyer should close it and take it along when leaving the room. Most laptops can be put in sleep mode rather than powering down completely, reducing the inconvenience and small symphony that accompanies powering up. If you do this, however, you need to close all your files and be sure that they are encrypted.

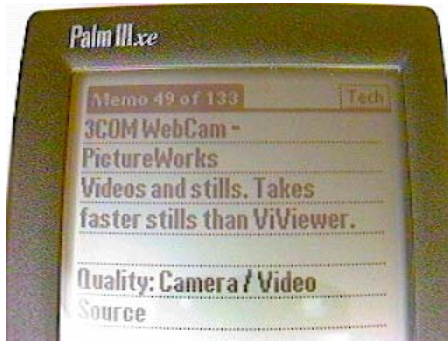
We again emphasize encryption: to protect the contents of a laptop, a lawyer should use a strong security program that encrypts at least the folders containing confidential information. You do not want others gaining access to confidential information if you are out of the room or if your laptop is stolen.

Chapter 14. Handheld Devices

Handheld devices typically are used to contain address books and calendars. With their increasing capabilities and increased storage, however, the possibility of having confidential information stored in a handheld unit (via memos, spreadsheets, or word processing documents) is very real. Given the small size and relatively low cost of a handheld unit, it is easy to lose them.

Handhelds offer a minimal level of security by allowing you to use a password to protect access to the unit. A person knowing the password can turn the machine on but not access any of the programs. You need to be aware, though, that the current Palm operating

system has enough holes in it that an experienced hacker using a laptop computer could crack the password protection easily.



Palm Organizer
Photo by Anderson

There is any number of programs that will allow you to encrypt the data on your handheld unit, but you will pay a considerable price in speed and storage to encrypt. Encryption on the handhelds isn't quite ready for prime time, although Palm says that the Palm OS 5.0 will have RC4 encryption.

We'll probably just have to wait and see how successful the changes to the handheld operating system will be. Different companies implement security with different effectiveness. Microsoft, for example, has a terrible reputation in the cryptographic community for improper

implementation of cryptographic protocols that are easily broken. There's a lot of snake oil for sale about security and encryption, so beware.

The easiest solution to protecting confidential information on a handheld device is very low-tech: just don't put anything confidential on your handheld. If you want to keep a list of your passwords or credit card numbers on your handheld, use a program designed to encrypt them, but don't try to encrypt the entire disk. Keep the confidential information in your laptop or desktop where it can be properly protected and encrypted.

Part III: Problems, Alternatives and the Future

Even though many of the potential conflicts and other problems of the shared office space can be avoided, there are still problems that are inherent within the nature of sharing office space with other attorneys. Potential conflicts of interest may arise if two different attorneys in the same office suite represent parties who are suing each other or are on opposite sides of a case or transaction. There is always the risk that you will be seen by the public as being in partnership with your fellow suitemates, which must be avoided at all costs. Further advances in technology may raise new problems. This part discusses these problems and offers a few alternatives to the shared office space.

Chapter 15. Potential Conflicts of Interest within the Shared Office Space

No jurisdiction in the United States has yet addressed the potential for conflicts within the shared office space. But just think about the following scenario:

Husband and wife are getting divorced. Each goes to a lawyer in the same suite at a different time. The lawyers, of course, don't communicate with each other about their cases, for that would be ethically improper. But how do you think the respondent spouse

will feel when served with papers bearing the identical address (though different phone number, perhaps) of that spouses own lawyer?

The worst part about this problem is that there's nothing you can do to prevent it if you share office space with other lawyers. You can't pre-check conflicts with them, because you might well be disclosing confidential information (i.e., the purpose of the client's visit) by so doing. Sooner or later—sooner in a small town, later in a big urban center—this will happen.

How such potential conflicts get resolved will in all likelihood depend on the physical layout of the office. Some commercial suites have individual suites off of a central interior hallway, but the lawyers' office and secretarial area are walled off from the rest of the firm. The common areas like the library, copying room, and conference room are open to all tenants of the suite, but individual tenants would have a very difficult time getting at each others files and confidential information. Under these circumstances, there is little chance that a court could find any likelihood, either in a malpractice case or in a motion to disqualify, that the secrets of one client could be compromised by close proximity to another lawyer...provided, of course, that you have followed the recommendations we have been discussing and have kept your files locked up and your computers secure.

Compare that scenario with a more typical office layout. The two lawyers in question have offices next to each other. They are subleasing space from the largest law firm in town, and one of the selling points of the suite is that the décor looks just like that of the big firm, even down to the open cubicles and ready access of files between one lawyer and another. If the lawyers have taken no steps to secure the confidentiality of their client's secrets, they are in serious trouble. True, it is difficult to formulate a disqualification theory under most rules of professional conduct, since the two lawyers are not members of the same firm. But it is easy to formulate a malpractice theory if confidential information gets leaked. Disciplinary violations can also be imagined, such as the lawyer's duty to keep inviolate, and at every cost to himself or herself, the secrets and confidences of the client.

We do not suggest that a shared office arrangement with other lawyers is inherently wrong. It is, however, inherently dangerous, even if the danger is latent rather than patent. To avoid the problems outlined in this chapter, you need to implement the security discussed earlier.

Chapter 16. Avoiding Ostensible Partnership

Occasionally lawyers band together to project to the world what appears to be a medium-sized firm, when in fact they are nothing but sole practitioners who shared expenses. They share a common firm name which appears on the door, on the "firm" letterhead, and on each lawyer's card. To all the world, they look like a law firm instead of a bunch of solos.

This is an incredibly dangerous and stupid arrangement for each of the attorneys. They have exposed themselves to liability for each of the errors and omissions of the others by a theory of ostensible partnership (sometimes called partnership by estoppel). While they

are not in fact partners, their presentation of themselves to the world as a law firm will estop them from denying that they were acting as a partnership.

That's only for starters. If they are individually insured, they will soon have coverage problems for misrepresenting the nature and scope of their practice to their individual carriers. Coverage may be denied entirely. Moreover, while the taxing authorities may not tumble to the arrangement, if they do the lawyers will be facing possible penalties for failing to file partnership tax returns and for additional income. If all the operating expenses and incomes are similar, that probably is not a big problem, but imagine what will happen if the feds or state decide to audit a year where one of the lawyers in the "firm" won a multi-million dollar case. Best of all, the other lawyers get taxed on money that they never received.

But there are also less obvious ways that a group of lawyers sharing an office space can create problems for themselves. Some lawyers like to share a phone and fax. While sharing a fax line will not create the appearance that the lawyers are acting as a firm, a shared phone line will, particularly if combined with a shared fax number.

Another area of potential trouble is how the lawyers present their business cards. Lawyers looking for business naturally like to get their cards into the hands of as many people as possible, and therefore will have the cards available at the reception area. If the lawyers all have different phone numbers and identify themselves differently (for example, John Jones has "Law Offices of John Jones" printed on his card whereas Fred Smith has "Law Offices of Fred Smith" printed on his), there will probably not be any confusion. However, consider the case where the cards simply have the name of each lawyer with a common phone and fax number. A potential client may well conclude that everyone is a member of the same firm since they share an address, a suite, a common phone line, and a fax. In short, you need to make it clear that you stand apart from the other tenants in your suite.

A related but distinct problem involves lawyers who share office space with other businesses or professions. The lawyer in such a case must take care to insure that there is no suggestion of any business relationship between the other businesses or professions in the suite. Failure to take such steps can result in civil liability or ethical censure.

Chapter 17. Of Counsel vs. Sharing Office Space

One common alternative to sharing office space is to become "of counsel" to another firm. An "of counsel" lawyer is typically defined by what the lawyer is not: not a partner or shareholder of the firm or lawyer to which the of counsel lawyer is of counsel, and not an associate (i.e., employee) of the lawyer or firm.

Financial arrangements between "of counsel" lawyers and the firm vary widely. Some have some income sharing and referral arrangements; others serve basically as tenants.

The advantage of becoming of counsel to a firm is that you avoid any possibility of the breaches of confidentiality outlined above. Because you already have a relationship with the law firm, there by definition can be no breaches of confidentiality, and all you have to remember is not to discuss your clients' cases in the conference room in front of an opposing lawyer.

To every upside there is, of course, a downside. The downside of the of-counsel relationship is two-fold. First, the potential for conflicts of interest is greater, and either the of counsel lawyer or the law firm is likely to be disqualified if they end up representing adverse parties. The of counsel lawyer and the firm are sufficiently close that they are unlikely to be able to represent opposing parties in a lawsuit or a transaction (at least without a written waiver by the clients after full disclosure), whereas two lawyers or firms in a shared office where the lawyers have adopted the suggestions above will probably not face such problems. Certain types of practice may also be more prone to such problems, such as family law.

The second downside is that of insurance. Most errors and omissions insurers demand full information of every lawyer who is a member of the firm or is of counsel to the firm, and insist that the of-counsel lawyers be insured under the policy. This requires fairly detailed disclosures, including financial data and claims history of the of counsel lawyer or firm. Further, the firm or the of-counsel lawyer may have a different premium structure, depending on how risky the practices are. (For example, a lawyer doing public offerings would dramatically increase the cost of getting insurance for a firm of criminal defense lawyers who have relatively little exposure. The reasons for such an of counsel relationship are not at all obvious; we give the example simply as an instance of how premium structures can vary and should be accounted for in considering the viability of an of-counsel relationship.) If you are not prepared to make such disclosures, an of-counsel relationship will not work for you.

Chapter 18. The future: Evaluating Emerging Technologies

The physical layout of a law office and the capital investment needed by a lawyer have changed dramatically since the mid-1970's. Before that, at least a couple of generations of lawyers had pretty much the same requirements: a typewriter for the secretary, a dictating machine and a transcribing machine for the secretary. A photocopier was nice, but many lawyers got by with carbons. Two telephones, one for the lawyer and one for the secretary, sufficed. The lawyer got all the information he needed from printed material, so sharing a library was advantageous since books, then as now, are expensive and occupy a lot of real estate. The major expenses were determined by the size of the spaces rented and the size of the library.

Fast forward to 1990. Now personal computers were required to get out the work, as were high speed laser jet printers. Lawyers needed fax machines, which were quite expensive, and could not live without a photocopier. Books were still the easiest way of getting information. Now the expenses of running a practice included the significant expense of keeping a photocopier operational and maintaining a fax machine. Each lawyer also needed a secretary with a computer, although printers, at least, could be shared between computers or even all around the office.

Now move to today. Fax machines and computers have become cheap commodities affordable by any lawyer. CD Rom and on-line services provide the libraries, thus freeing up valuable space for other uses. Keeping a photocopier happy and operational is still as expensive as ever, and most lawyers find high-speed Internet access (which is also

expensive) desirable. New technology—scanners, mass storage devices, presentation software and projectors—require an ever greater capital budget for the individual lawyer.

And who knows what the future will bring? All we can be sure of is that it will bring new technology. The price of that technology may drop over time (like faxes, computers, and modems), or may remain constant (like the photocopier). It may wax and wane: CD towers for legal libraries became popular in the mid-1990's and were very expensive (thus being an attractive feature for a shared office space), but have been practically wiped out by Lexis and WestLaw which have finally offered sensible pricing policies for on-line research

Whenever a new technology is introduced, it will probably be expensive. If so, it makes sense to split the cost of that technology by spreading it among as many people as possible. Whether you are a tenant in a shared office suite or the landlord, identifying and providing such potential benefits and savings is an important part of having an effective and efficient office.

At the same time, every lawyer who shares office space with other lawyers needs to consider carefully the problems faced by each new technology. When the fax first became popular in the late 1980's, none of the precautions we describe here were taken, for the simple reason that there was no practically way to do it and still have the value of a shared fax machine. This in no way lessens the ethical problems we have described with the compromise of client confidentiality. Future technology may present similar problems.

All the careful lawyer can do is to be prepared. Analyze whether the new technology will expose your clients secrets to people outside your firm. As with liberty, the price of technology in terms of client confidences is eternal vigilance.

Conclusion

There is nothing inherently wrong with sharing office space. It permits you to buy more physical plant and services per dollar than you could on your own, particularly if your firm has fewer than five members.

What must remain in the forefront of your thoughts, however, is the fact that you do not control all the space you work in. You may trust your suitemates, but can you trust all of the people in the suite all of the time? Even if you can, your savvy opponents could take advantage of your security oversights and compel disclosure of your work product and information that you thought was privileged.

Share your suite, but not your clients' confidences.

Other eBook Formats

This electronic book is available in other formats. Please visit the Web sites of either author, Wells Anderson and Joe Hartley, to download *How to Protect Client Confidences in a Shared Office Space* in another format. www.wellslegaltech.com www.hartley.com

Photo Credits

Versions of this eBook that support graphics contain color photographs and images.

AEC photos courtesy of American Executive Centers, which serves practices of all sizes in Pennsylvania and New Jersey. They offer private offices, space for support staff, office services and occasional office space or conference rooms.

Tel: 800-736-6034

Web: <http://www.aecphilly.com>

C & E photo courtesy of Cressy and Everett, Mishawaka, Indiana, Tel: 574-271-4060

Additional photos courtesy of www.rogersgifs.com and www.openimage.net

Feedback

We encourage you to write to us with your reactions, suggestions, corrections, praise and criticism at:

Wells Anderson wa@wellslegaltech.com

Joe Hartley jmh@hartley.com

Checklists, Suggestions, Bibliography

Additional information is provided below in the Appendix.

Appendix

Appendix 1

Lawyer's Shared Office Checklist

- Rules of behavior (to be included in the office procedures manual)
 - No talking confidential matters in the halls or outside the office
 - Client conversations take place only behind closed doors
 - Close door or lower voice during office phone calls
 - Keep confidential materials inside of office
 - Take care in talking to the staff outside of attorneys' offices
 - Take phone calls from clients only in attorney offices
 - Photocopying: no one leaves the common machine unattended
- Phone calls
 - No client messages left with receptionist
 - No client messages left with other secretaries
 - Taken by staff in low voice
 - Answering machine/voice mail
 - Proper passwords?
 - If answering machine, locked away?
- Fax: no shared fax
 - Fax secured in closet or box
 - Fax card in computer
 - Fax in attorney's office
- File storage
 - No storage with other tenants
 - Stored in attorney's office?
 - Door locked?
 - File cabinets locked?
 - Stored in secretarial area
 - Cabinets locked
 - Separate, lockable storage area?
- Work Product
 - Locked up after work
 - Mail in attorney's office
 - Work in progress—locked up?
 - Filing
 - Chron files
 - Phone message pads stored
- Shredding
 - All drafts shredded or placed in file (procedures manual)
- Individual computers
 - Password protected
 - Centralization of passwords used by staff and attorneys

- Encryption?
- Network security
 - Passwords
 - Internet connections
- Laptops
 - Encrypted
- Handhelds
 - No confidential information
 - Password protected access

Appendix 2

Suggestions for Law Firms Renting Space to other lawyers

Describing what to look for as a tenant is somewhat easier than determining what a landlord or sublessor should offer to the market. That is more of a business decision than a legal problem.

Any firm that wishes to rent out excess offices faces some difficult decisions. If the subleasing lawyers are given free run of the firm, then the subletting firm *must* insure that its own files are under lock and key. It cannot offer a common file room. By subletting space without restricting access of the subtenants, it exposes itself and its tenants to breaches of confidentiality.

Some subletting firms have actually walled off the office areas they sublet. As part of the rent, they supply and service a separate photocopier and coffee room. This does not prevent problems for the subtenants, who still have to take all the precautions we have discussed. It does, however, relieve the subletting firm of having to take the same precautions within its own offices.

Walling off the subtenants also creates problems when the subtenants need access to shared facilities that are included in the rent. By planning the space well, the subletting firm can put enough conference rooms in the area that is being subleased that the subtenants do not need access to the firm's conference rooms. The library, though, creates problems, since one of the driving factors for lawyers subletting space is to avoid the cost of a full library. Some firms have solved this problem by designing the library so that it can be easily accessed, but wall off the remainder of the firm. This, of course, is inconvenient for members of the firm, who have to carry keys or magnetic cards to gain access to their own libraries. If the paper library becomes a thing of the past with on-line services, this concern will abate. Meantime, the subtenants must be given access to the library while not permitting them to roam the halls and file rooms of the firm at will.

One of the features which would make the sublet office space extremely desirable would be the equivalent of a walk-in closet where subletting attorneys could store their files, place their fax machines, and even place a computer server so that it could be secured by closing and locking the door. Unhappily, modern design seems to favor shrinking secretarial areas instead of reconfiguring them to provide for secure use. If lawyers become aware of the potential compromises to client confidentiality in the typical layout, such a feature would be a persuasive selling point to prospective subtenants.

Bibliography

Protecting Electronic Data in the Shared Office Space, W. Anderson and J. Hartley, GPSOLO, December 2001, General Practice, Solo and Small Firm Section
<http://www.abanet.org/genpractice/magazine/dec2001/andersonhartley.html>

How To Protect Client Confidences in a Shared Office Suite, W. Anderson and J. Hartley, Law Practice Management Magazine, March 2002
http://www.abanet.org/lpm/magarticle2002_v28n2_p38.shtml

Opinion No. 303 – Sharing Office Space and Services by Unaffiliated Lawyers, District of Columbia Bar, Legal Ethics Committee
http://www.wellslegaltech.com/www.dcbbar.org/attorney_resources/opinions/opin303.pdf

Sharing of office space and facilities with non-lawyer business, Illinois State Bar Association, Opinion No. 90-6
<http://www.isba.org/CourtsBull/EthicsOpinions/90-06.asp>

Rule 126, The Law Society of Alberta
http://www.lawsocietyalberta.com/Info_lawyers/forms/5-1.asp

On Risk Management: Avoiding the Pitfalls of Office Sharing, K G Kenny
http://www.legalmutual.com/newsletter_onrisk5.html