



*State Bar of California Annual Meeting
September 2008*

**Secret Life of PDAs
Protecting Client Confidentiality
Under Rule 3-100
in the
Context of Mobile Technology**

*Lisa Miller, Esq.
Miller Consulting*

(818) 508-8502 / Lisa@LMillerconsulting.com

*© 2008, Lisa Miller, Miller Consulting
All Rights Reserved*

Greatest ethical imperative: protect client confidentiality.

Comply with Rule 3-100!

Most law firm employees connect from out-of-office locations via mobile technology

Client confidences are present / accessed through personal digital assistants

No rules yet specifically addressing Rule 3-100 and PDAs.

Responsible counsel: take reasonable steps to protect client confidences

I. State Bar Requirements Regarding Client Confidences

Almost absolute obligation: maintain confidentiality

Rule 3-100: Confidential Information of a Client

A member shall not reveal information protected from disclosure by Business and Professions Code section 6068, subdivision (e)(1) without the informed consent of the client

Business and Professions Code section 6068, subdivision (e)(1), it is a duty of a member: "To maintain inviolate the confidence, and at every peril to himself or herself to preserve the secrets, of his or her client."
involves public policies of paramount importance

Confidentiality, trust: hallmark of the client-lawyer relationship. Clients encouraged to seek legal assistance, must communicate fully and frankly, even as to embarrassing or legally damaging subject matter
Counsel needs information to represent the client

Client-lawyer confidentiality: attorney-client privilege, the work-product doctrine and ethical standards of confidentiality.

Confidentiality rules apply to information relating to the representation, whatever its source

Neither State nor local bars have produced opinions regarding protecting client confidences in the context of mobile technology; the issues are in the works, so decisions / guidelines are coming
Take steps now: don't get caught by mobile technology threats in the context of protecting client confidences; implement coherent, firm-wide policies

II. Threats to PDA Security

PDA's often contain / can access confidential client materials, attorney work product.

Mobile wireless devices (including PDA's): the weakest link in security
Law firm employees with PDA's extend the edge of the law firm network to risky areas

Two challenges when striving to comply with Rule 3-100:

- Enforcing law firm PDA security policies in pervasive wireless networking environments
- Securing the law firm mobile workforce from the rising threats and attacks that happen outside the office

PDA devices face a number of threats:

1. Theft
2. Unauthorized Access
3. Electronic Eavesdropping
4. Modification of Data

Methods for preventing access:

- Encryption
- Authorization
- Authentication

5. Hackers

- A. Evil Twin
- B. Wi-Phishing
- C. Man-in-the-Middle Attacks
- D. Ad-Hoc Connections
- E. Municipal WiFi Threat

1. Accidental associations of the law firm's wireless users to municipal WiFi access points

2. Employees circumventing wired content filtering and internet access monitoring technologies installed at the office by connecting to available municipal WiFi access points

3. Increased attack vulnerability from hackers on the municipal WiFi network through Evil Twins and Wi-Phishing

More sophisticated PDAs = more confidential information passing through the device, such as desk-tops, where client confidences are stored.

Keep informed of threats

III. PDA Protective Processes

Implement protective processes: safeguard client information, meet obligations under Rule 3-100

Personal Data/Digital Assistants (PDAs)

Risk leaking confidential client information, violating Rule 3-100.
Small, easy to steal, frequently used in public, sync with the law firm's desk-top computers (a potential gold-mine of information for unscrupulous users)

Users check e-mail, surf the Internet, and other tasks: When use PDAs for online tasks, devices become vulnerable to exploitation.

Biggest threats:

- Password theft
- Data theft through line sniffing
- Theft of the PDA itself
- Mobile code vulnerabilities
- Wireless vulnerabilities

Biggest security risk: theft of the device - securing the data on the device in “stand alone” mode is the best precaution. End-user compliance with security protocols is key. (Wireless vulnerabilities only affect PDAs that use wireless services or have their wireless ports enabled)

Encryption options: secure data, links to communicate with remote systems and networks, typically one of two types-

- Secure the data: PDA in “stand-alone” mode
- Secure the link: data moves back and forth to and from law firm devices (desktop unit that it uses for hot-syncing)

Encryption product to secure either the link to the desktop hot-sync system or for wireless surfing: wrap PDA traffic in a VPN (protects data in transit)

Security policies: protect confidential data on PDAs

Disable the wireless port: reduce the risk of sensitive data transmitted to unauthorized individuals

End-user behavior policies: PDAs may not receive/send e-mails with confidential information.

Except for PDA security products related to hot sync functions, most of the PDA security products on the market are similar to security products for desktop systems:

- Authentication
- Encryption products
- Anti-virus products
- Password products

Implement password enforcement product: require all PDA users to supply a password for authentication

PDA's typically operate in "always on" mode: PDA's are never completely turned off (if battery removed, device loses data)

To ensure that wireless transmissions related to client confidences are protected and not leaking into wireless access point that counsel may not know about, attorneys can put PDA devices into an electromagnetic shielding bag while carrying them around. Under \$100/PDA.

PDA's with confidential client information: install "bit wiping" packages - entire memory is over-written, reformatting or completely erasing the stored memory. Data is wiped away: can't be recovered. Consider setting bit-wiping processes to kick in if PDA not synchronized within a set timeframe/too many bad password attempts.

If counsel allows PDA's on the law firm network infrastructure, counsel needs security controls and policies to keep these devices from damaging confidential information under Rule 3-100.

If the law firm does not have security controls or policies in place for PDAs, keep them off the law firm network until counsel implements policies and security controls.

Eight Ways to Secure Law Firm PDAs and Comply with Rule 3-100

1. Physical Security

Keep PDAs properly stowed while traveling. Don't leave PDAs in jacket pockets or external pockets of baggage.

2. Software Security

Use a password to prevent unauthorized access and help prevent unauthorized access to the law firm's network. Use passwords properly, select them wisely, and keep them private.

Use software programs to prevent access to specified programs or lock a PDA up if it detects too many failed attempts to access either the device or the PDA operating system

3. Wireless Security

Whenever accessing a wireless network with a PDA, enable all safety protocols and ensure a secure wireless connection.

4. Data Encryption and Protection

Encrypt client data through appropriate software. Use removable storage cards (if possible) to prevent compromising confidential data if the PDA is stolen. Keep removable storage media in a separate location from the PDA when not in use while traveling.

5. PDA Anti-Virus and Firewall Programs

Just as anti-virus and firewall programs should be used on law firm laptops, they should be used on the law firm's PDAs.

6. Disable Bluetooth and WiFi

Disable the software whenever counsel isn't using the wireless connections, so that no unauthorized connections occur. In crowded areas such as airports and convention centers, it is impossible to know who may be seeking out devices to wirelessly connect and steal confidential data.

7. Monitoring and Detection Software

Use programs to monitor and detect activity on law firm PDAs, notifying counsel if someone is attempting to access programs on counsel's PDA or has made changes to the data on the PDA.

8. Use E-mail Wisely

Set up e-mail on law firm PDAs to filter spam and not open executable files received by e-mail.

Law Firm Privacy Policies for Clients

Privacy Policies at law firms should cover at the least the following points:

I.

What this privacy policy covers –

E-mail and other electronic communications can be inherently insecure

II.

Information collection and use –

What the firm does to protect clients and clients' confidences

What clients are expected to do to protect their own confidences

Examples of what might or could happen if clients do not help protect their own confidences

III.

Information Sharing –

Disclosure situations and possibilities, with examples

IV.

Confidentiality and security-

List of steps the law firm has implemented and takes regularly to protect client confidences in the context of mobile technology

List of steps the client is expected to take to help the law firm protect the client's confidences

Examples of possible negative results from clients' failure to abide by the firm's mobile technology security policies

V.

Changes to the law firm's mobile technology privacy policy

Based on technology changes, court decisions, ethics decisions and other governing rules and regulations, the law firm will be adjusting its mobile technology security policies from time to time and will notify clients of these changes in writing to provide maximum protection for clients and client information.

Law Firm Internal Policies

Mobile Technology Security for Smaller and Mid-sized Law Firms

At a minimum, law firms should develop a policy regarding mobile technology security that includes the following:

I. PDAs

- Passwords must be changed regularly (at least quarterly, if not more frequently)
- The firm should perform random checks of mobile technology devices to ensure that password protection is in place and has not been turned off or otherwise bypassed
- The firm should keep records of these inspection checks to help it ensure that these safeguards are in place
- Law firms should warn users of mobile technology about “Shoulder Surfing” in the context of password use.

- Use a PDA remote wipe-out process if a PDA is lost or otherwise compromised
- The law firm should use encryption at all times. This requires that it check the wireless carrier it is using to ensure that encryption is being used. Smaller wireless companies in California, especially in central California, might not be encrypted. In this situation, PDAs will not be protected when in use and the law firm should not allow any use of the device in this circumstance. This is most likely to occur when the lawyer is in “roaming” mode. While Blackberries should encrypt automatically, telephones do not.
- Law firms should be aware that the Internet is not a Common Carrier, so it does not have any protections under Title II.

II. Laptops

- Law firms must require that all users of mobile computers use passwords, no exceptions. Passwords must be changed quarterly, at least, through forced changes. (No remote wipe-out process is available)
- Law firms should use VPN-IPSEC, the most secure protocol, for encryption
- For remote accessing of the law firm's network from other computers, the law firm should consider restricting IP addresses with permission to access the law firm network. For example, IP addresses of counsels' homes would be permitted access to the law firm's network, but this would bar access from Internet cafes and lounges.

III. General considerations for law firm mobile technology security

- Clients should be required to initial every page and sign the last page of the law firm's mobile technology security policy. Moreover, clients should separately sign a declaration contained in the policy stating that the client wants the law firm to communicate with the client electronically. The client must then register an IP address for law firm communications.
- If the client does not opt into the firm's mobile technology security policy, then the client has not agreed to e-mail communications. It is the law firm's responsibility to put the client's e-mail address on a "Black List," so that the law firm's system will automatically reject e-mail from the client's IP address (this process is similar to a spam filter).

Retainer Agreement Considerations

Law firms should consider including the following overarching concepts in the retainer agreement:

I. The Big Picture

- Use simple language. Clarity is key.
- The retainer agreement is more than a legal contract; it is a guide to behaviors that protect the attorney-client relationship.
- The goal is to manage client expectations as well as counsels' expectations.
- The retainer agreement should include a Best Practices statement for the client, and include acknowledgement of receipt by the client.

II. Attorney Responsibilities

- Counsel should anticipate use of technology in the attorney-client relationship and address the communications in this relationship in these terms. The agreement is a living document as to new clients. AS to current clients, mutual agreement is required to modify the agreement. Counsel should update the retainer agreement to reflect technological concerns as often as necessary.
- Counsel should ensure that the retainer agreement addresses the current manner in which the client and counsel communicate.
- Regarding existing clients, who already have signed retainer agreements, counsel can send a letter when the firm changes any aspect of its mobile technology policies or procedures, advising the current client of issues that the client should consider in communicating with counsel from or to remote mobile devices.
- Counsel expects that the client will be truthful with counsel.

- Counsel should list the aspects of mobile technology security for which clients are responsible. This includes the manner in which clients can help maintain their own secrets and confidences
- Retainer agreements should include a statement that the client will make best efforts to follow the mobile technology practices of the law firm.
- Counsel should anticipate that clients will be using e-mail and sharing computers.
- Be clear that clients may not copy anyone on their e-mails or forward the law firm's e-mails to any third parties without first discussing this with the attorney.

- If the client shares the computer with a third person, the client must advise the attorney if the client is sharing password protected e-mail files, to help protect the attorney-client privilege and ensure confidentiality.
- More sophisticated clients will expect higher levels of IT protections than less-sophisticated clients.
- Counsel should include a “confidential Communications” tag in the subject line, at the top, and as the bottom paragraph of e-mail communications.

III. Client obligations

- Clients should use the phrase “Attorney-Client Privilege” on the first line of e-mail communications with counsel.
- If the client shares a computer, the client is responsible to take steps to effectively shield attorney and client communications from access by unauthorized and unnecessary third parties. As part of intake procedures, the law firm should specifically ask the client if the client shares a computer or if anyone else has access to the computer.
- Clients should be required to use passwords on all mobile communication devices and shared computers
- When the client uses a mobile device provided in a public place, such as an Internet café or Internet lounge, the client must be instructed to and be required to erase the cache, erase passwords, and erase the history when logging off.