BARCLAY DAMON LLP

The Ethics of Cybersecurity in Virtual ADR

Kevin D. Szczepanski

Partner, Co-Leader, Cybersecurity Team,

Barclay Damon LLP

What's driving the pivot to virtual communications?

- COVID-19
- Convenience
- Costs

Today's Discussion

- Ground rules
- Key takeaways
- Good cyber "hygiene"
- Virtual ADR Recommendations
- Additional Considerations for Clients

The Ground Rules

- Rule 1.1 – Competence
- Rule 1.4 – Communication
- Rule 1.6 – Confidentiality

Rule 1.1 – Competence

- A lawyer should provide competent representation to a client."
- "Competent representation requires the legal *knowledge*, *skill*, thoroughness and preparation reasonably necessary to the representation."
- **Comment [8]**: "To maintain the requisite knowledge and skill, a lawyer should . . . (ii) keep abreast of *the benefits and risks associated with the technology the lawyer uses to provide services* to clients or to store or transmit confidential information[] . . . ."

Rule 1.4 - Communication

- “A lawyer shall . . . . Reasonably consult with the client about the means by which the client’s objectives are to be accomplished[]”
- “A lawyer shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation.”

Rule 1.6 – Confidentiality of Information

- "A lawyer shall make *reasonable* efforts to prevent the inadvertent or unauthorized disclosure or use of, or unauthorized access to, information protected by Rules 1.6, 1.9(c), or 1.18(b)."
- In determining what's reasonable, several factors are considered:
    - The sensitivity of the information;
    - The likelihood of disclosure if additional safeguards are not employed;
    - The cost of employing additional safeguards;
    - The difficulty of implementing the safeguards; and
    - The extent to which the safeguards adversely affect the lawyer's ability to represent clients (*e.g.*, my making a device or software excessively difficult to use).

Key Takeaways: A Lawyer Must. . .

1. Understand the benefits and risks of technology.
2. Disclose them to the client.
3. Obtain the client's informed consent.

When: at the beginning of the engagement, or before a new technology is used.

How: in writing ("If it's not in writing, it didn't happen.")

Getting Started: Good "Cyber Hygiene"

- Conduct a **Cybersecurity Risk Assessment**
  - What data do you have?
  - Do you need it?
  - Where is it kept?
  - Who has access to it?

Implement Reasonable Safeguards

- Secure Wi-Fi Connection
- VPN
- Multi-factor authentication
- Access controls
- Limitations on use
- Firewalls
- Anti-malware, -spyware, -virus software
- Security patches and updates

Test and Train

- Vulnerability scans
- Penetration testing
- Training

Develop an Incident-Response Plan

- Know what to do when a cyber incident happens
  - Breach coach
  - Forensic team
  - Cyber-insurance coverage

Virtual ADR - Recommendations

1. Remove the platform's **terms of service** and **privacy policy**.

Virtual ADR - Recommendations

2. Consider implementing a **written confidentiality and information-security agreement**.

Virtual ADR - Recommendations

3. Create a random, or randomly selected, **meeting number** for each session, and **password protect** each meeting.

Virtual ADR - Recommendations

4. **Manage participants** by limiting attendance, removing unauthorized participants, and locking sessions.

Virtual ADR - Recommendations

5. **Ensure that sessions are not overseen** by anyone in the household, office, or other remote location from which each party is participating.

Virtual ADR - Recommendations

6. Employ a **“clean screen” policy.**

Virtual ADR - Recommendations

7. Secure sensitive **documents**, session **recordings**, and **transcripts**.

Virtual ADR - Recommendations

8. Require **vendors** to comply with reasonable cybersecurity safeguards.

Considerations for Clients

- Discuss the nature and extent of the client's safeguards.
  - Secure Wi-Fi, VPN
  - Private location
  - Use password-protected link if possible
- Consider the client's comfort level with the technology.
- Challenges may require *avoiding* virtual technology.

Summing Up. . .

- Virtual ADR requires a commitment to cyber hygiene.
- Conduct a risk assessment.
- Implement a cybersecurity policy and an incident-response plan.
- Understand and communicate the benefits and risks associated with virtual technology.
- Meet, confer, and agree on appropriate safeguards for virtual ADR sessions.

Questions?

Selected Sources

- Formal Opinion 498, Standing Comm. on Ethics and Professional Responsibility, American Bar Assn, Mar. 10, 2021.
- Formal Opinion 754-2020, Comm. on Professional Ethics, New York County Lawyers Assn.
- "Cybersecurity Alert: Tips for Working Securely While Working Remotely," Technology and the Legal Profession Comm., New York State Bar Assn, Mar. 12, 2020.
- "Privacy Considerations When Using Zoom," UC Berkeley Office of Ethics, https://ethics.berkeley.edu/privacy-considerations-when-using-zoom.
- Steven A. Certilman & Eric W. Wiechmann, "ADR in the Age of Cybersecurity," *NYSBA New York Dispute Resolution Lawyer*, Spring 2019, vol. 12, no.1.
- Krishna Jani & Donna Urban, "Tips on Protecting Your Virtual Meetings to Avoid a Cyber Security Breach," jdsupra.com, Apr. 13, 2020.
- Ellen Rosen, "The Zoom Boom: How Videoconferencing Tools are Changing the Legal Profession," www.americanbar.org, June 3, 2020.
- Kevin D. Szczepanski, "The Ethical Obligation of Cybersecurity," *Buffalo Business First*, Sept. 6, 2017.