Rosenblum Newfield, LLC

Attorneys and Counselors at Law

Digital Data Policy and Procedures Checklist:

Steps, Issues & Resources

NYC
(212) 888-8001

White Plains
(914) 686-6100

Connecticut
(203) 358-9200

Contents

Digital Data Policy & Procedures Checklist: Steps, Issues & Resources

Privacy and security policies for digital data – sometimes referred to as cyber liability or data breach – have existed for years. However, as digital resources become more complex, with new equipment, remote servers (referred to as "the cloud"), off-site back-up storage, and so-called BYOD (bring your own device) technology (staff using their own equipment rather than office supplied equipment), new issues arise. HIPAA provided a significant amount of guidance for "information policies" for health care providers. However, as extensive as HIPAA is, the regulation is designed to protect patients, and it creates regulatory burdens, which require compliance. However, it is only part of the digital data safety net, something that businesses in all areas of commerce must consider.

We are providing the following information and resources based on its professional expertise, using the experience of developing cyber policies and procedures for the firm as an example. The purpose is to outline general steps to consider in putting digital policies in place. The intended result is to minimize risks of cyber disasters that can occur if proper procedures and protections are not in place. These can include:

- Inadvertent loss or destruction of digital data
- Unwarranted intrusion and theft of digital data.

We will also explore insurance coverage which may be applicable in the event of a cyber situation.

Rosenblum Newfield undertook development of its own cyber policies for a number of reasons bulleted below that may very likely be applicable to our clients and colleagues as well.

- Such policies are part of proper office management. They are especially important for offices with sensitive information and, as a law firm representing individuals and companies, we do maintain and transmit sensitive information.
- We want people who work for us and with us to respect and help us promote these policies and to let us know if they have special concerns in this regard.
- Concerns about preservation and securitization of data is a constantly evolving challenge. These guidelines provide a framework for today and for future changes.
- We want our clients, now and in the future, to know that we are familiar with cyber-liability policies and can assist them with their policy development. Health care providers are, of course, familiar with privacy and security mandates from HIPAA. However, the field is continuously evolving. Technology (for example, use of personal devices like smart phones) is changing. There is increasing availability of insurance for cyber losses. Therefore, the policies and related solutions need to be updated.
- By enlisting the expertise of a tech staff up-to-date with the latest innovations in cyber protection (firewalls, anti-virus and encryption software) we are advocating for entire policy and technical systems designed to enhance protection of the data entrusted to us, increases confidence of those with whom we serve and provide guidance to our staff and those with whom we work and communicate.
- We are proactively working to stay current with evolving business best practices and are encouraging our colleagues and clients to do the same.

Defining "Cyber"

The adjective "Cyber," like "the Cloud" and other terms in today's technology glossary, is intended to help make intangible concepts more concrete. The term "Cyber" refers to the invisible bits of data transmitted on telephone or cable lines and through the airways. It is a term used to reflect the types of non-traditional data that we have the ability to transmit and receive today. The term 'Digital Data', as we use it in this document, is a synonym for 'Cyber Data'.

There are various types of digital data may be treated differently for purposes of protection and establishing policies. Some of these are:

- Telephone calls (which may be transmitted over the internet and which may be intercepted even if on traditional telephone lines)
- E-mails, which may include documents, case files, and internet searches
- Information saved on office computers.
- Information saved on remote, third-party servers (in the Cloud)

Cyber risks

What risks are associated with digital data and communications? The risks are that sensitive, personal information is inadvertently lost or corrupted, inadvertently transmitted to those who should not have received the information, or stolen by those who should not have access to digital data and may use it for nefarious purposes. The major cyber risks also refer to the risks associated with digital information including unintentional loss, unintentional transmission to third parties, theft and failure to comply with extensive and evolving regulation.

The Best Defense: Technology

The best defense to intrusive or defective technology is better technology. It is a precondition to any meaningful insurance coverage. It includes solutions like firewalls, encryptions, high security e-mail, and meaningful use of passwords.
In that regard, our firm uses a leading digital security company that:

- Audits the technology we have in place
- Reviews our digital security procedures
- Assesses the level of vulnerability (or invincibility) our equipment provides and offers plans for maintaining state of the art solutions.
- Provides a comprehensive report for internal use and for use in the remote event of third party claims.

We have also vetted a list of reliable, knowledgeable digital security firms, which we provide to our clients and interested parties on request as part of our services. We have no financial arrangement with any of these vendors.

The Importance of Cyber Office Policies

As a firm, we do whatever we reasonably can to avoid loss or disclosure of digital data. Our clients do the same. That is a given if one is a "business associate" handling sensitive health care information subject to HIPAA and/or the Health Care Affordability and Accountability Act. However, statutes requiring privacy and security require that subject entities have policies and procedures and ensure that they be enforced. Policies and procedures also provide a check-list to help entities fulfill their goals.

What Cyber Policies Do We Need?

Today we need cyber policies to address the following:

- What technology is in place to prevent accidental destruction / erasure of data?
- What procedures are in place to prevent inadvertent loss or transmission of data by office staff?
- What technology is in place to prevent theft of data, i.e., breach?
- What policies are in place to deal with breach or if accidental disclosure occurs?

Policies to deal with breach

As a small law firm, we are simply not the type of target for 'cyber attack' that large corporations – e.g., banks, defense contractors – or governmental entities are. Therefore, it is unlikely that policies for data theft will have to be implemented. However, inadvertent disclosure is a risk that every organization faces, regardless of its size. Everyone has heard of government employees in sensitive positions who have lost laptops. Even if part of the risk our company faces may be small, we addressed it in our policies. It is still good to know what to do if disaster strikes, not only because it is a good business practice to be prepared, but also because it helps us to advise clients who are in greater need of this information.

Following are some steps and related issues to consider in the event of a breach:

- It is critical to notify those individuals and entities affected or involved that there has been a breach of security and possible or actual disclosure of confidential data.
- Sensitivity is needed to ensure that the disclosure does not compound the problem by publicizing the fact that security has been compromised. For example, it may be difficult at first to determine how extensive the loss has been. Determining this may be priority one. Similarly, if there is no reasonable likelihood of public disclosure, such information is significant. If there is clear likelihood of harm, it may still be difficult to know the extent of the harm.
- The goal is to provide reasonable disclosure of likely consequences based upon the information available.
- Timing of notices is also a sensitive issue. Premature disclosure may cause more distress than timely disclosure. Therefore, timing of disclosure has to be evaluated in light of the known or reasonably expected circumstances and significance of the disclosure.
- It may be necessary, or even just helpful, to notify governmental agencies with potential jurisdiction, including divisions of consumer or cyber protection in offices of state attorneys general. The Federal Trade Commission and the FBI might be appropriate depending on the breach.

It also is necessary to notify insurers that may protect against such loss, including those providing coverage for Directors and Officers Liability, Business Interruption, Crimes, Employment Practices and General and Professional Liability.

Policies to Prevent Inadvertent Loss

Key policies to prevent inadvertent loss of data are:

- Personnel Policies – These include careful use of laptops, tablets, cell phones. Successful personnel policies depend upon humans being diligent and, perhaps, the correct word is hyper-vigilant. For example, when attorneys are in court, they are pre-occupied with clients, courtroom personnel and the subject matter of cases and without a policy-driven awareness of the issues be less careful about keeping equipment under their control.
- Password Policies – An important approach to avoid inadvertent loss of digital data is to have effective password protection. Effective passwords have a minimum number of units and incorporate letters, numbers and symbols. Your policies should educate employees about how to create and store secure passwords and require use of password best practices.

Technology to Prevent Inadvertent Destruction of Data

Policies for Digital Data protection are essential part of comprehensive planning.

Computer Back-ups – Computers crash, memory drives fail and power outages and surges can destroy or compromise digital data. Therefore, regular back-ups are essential. Traditionally, daily tapes were made and put in off-site safes. Today, the best approach is to have off-site, automatic and frequent back-ups where the data is located not only in locations that are as secure as possible, but also in diverse, secure locations. This is not necessarily back-up in "the Cloud". The Cloud generally refers to off-site servers, i.e., central computers with software and data of the sort that used to be housed in corporate or business offices. It is like calling on a consultant based in a branch office rather than an office down the hall.

Duplication of data/Redundancy is also important valuable. Thus, documents we use are contained elsewhere as follows:

- Pleadings, motions and some discovery is located on court web sites in Connecticut. This dramatically reduces the need for paper files.
- Reports are sent to insurers who maintain secure files.
- Medical records are maintained by providers.
- Other types of discovery, e.g., employment records, can be obtained. Obviously, if data for one case is eliminated, it is still a challenge to reconstruct a file. If data for many cases is lost, the job of reconstruction is substantial.

Technology to Prevent Breach

In order to understand ways of minimizing cyber risks, it is necessary to understand some of the technology that should be in place.

- Virus protection software is essential.
- Firewalls – software that keeps internal and external Internet connections separate – are essential.
- Telephone calls can be transmitted on a separate line than e-mail.
- E-mail can be on a separate line than Internet connections.
- Digital case files can be transmitted on a separate line.
- Encryption involves turning communications into code which can only be unencrypted by those who own the data.
- Some types of e-mails are sent through servers which are more secure than simply across the internet, i.e., Hotmail, Gmail, MSN and Yahoo!. On the other hand, this adds more steps to sending and opening making it less simple than traditional e-mail.
- Digital data transmitted through traditional lines are subject to hacking but are generally more secure that wireless data. The risk of disclosure is minimized by encryption. Increased use of smart phones and tablets reduces the ability to secure data but their use is inevitable.

Contracts with Technology Vendors, IT experts

You should have contracts with reliable digital vendors for procedures such as automatic digital back-ups to remote locations. Contracts should cover both duration and cost. In addition ask the following questions:

- How does the vendor address potential liability?
- Can they provide instant back-ups if on-site data is lost?
- What happens if they lose data?
- How will they stand behind their promises of security?
- Do they compensate beyond what many vendors describe as “the cost of the data” as opposed to the value of the data or damages associated with loss?
- What happens if data that is initially transmitted to point “A” is then transferred to other locations like an earthquake zone or an area fraught with hurricanes. Is there still protection in place? In most cases this is not automatic.
- Does the vendor share your concerns about privacy and security.
- Do they address these issues in their own policies and contracts?
- Are they pursuing “cost-effective” solutions at the expense of privacy and security?

Asking and obtaining satisfactory answers to these questions is critical to putting the right digital security partner/s in place.

Technical Support If Unwarranted Breaches Occur

Technical experts may help to evaluate and/or minimize risks. Some companies can evaluate who may have stolen data and how it may have been stolen. Other companies may help to notify those affected. Other companies may help to provide follow-up monitoring (e.g., credit ratings, identity issues) if necessary.

Insurance for Cyber Risks

Can you use insurance to mitigate risk and loss from theft or accidental disclosure of digital data? This depends. Some companies have pursued coverage under general liability policies. Some have pursued coverage under business loss insurance. Some have coverage for breach of digital systems. Meanwhile, some entities have broader cyber-coverage addressing the various risks described above.

Everything is potentially insurable – at a price. What is the right price? What are the damages sustained by third parties for wrongful disclosure? What is the cost of simply notifying clients of wrongful disclosure or loss? These are obviously difficult to calculate. Fortunately, insurers with expertise in these areas may provide guidance in this regard.

What insurance policies cover cyber-risks? As indicated, potential sources of coverage may include general liability and business interruption insurance. However, insofar as digital events represent new types of losses, it is not clear whether these traditional policies will cover such losses absent review of the specific policies.

A major issue for companies is the extent of coverage for property and/or business loss – so-called first party coverage – and third party loss for negligence. As indicated above, the cost of simply notifying the owners of the data may be substantial even if no harm results.

How is insurance priced? This is evolving as more insurers go after this "space" and competition increases. One approach is to consider the number of records or the amount of data stored.

Damages for Cyber Liability

For many companies, disclosure of information is probably inconsequential. After all, information about litigants in court is potentially public information, although it is rarely spread over the Internet absent some newsworthy aspect. However, regulatory penalties, for such acts as deceptive trade practices, may result in statutory fees and assessments of legal fees.

Risks to credit may be addressed by monitoring and may not materialize. However, identity theft is extremely damaging. Reputational damage is potentially unlimited. It is doubtful that any insurance policy (at any reasonable price) can fully compensate one for reputational loss. However, they can provide some compensation. All of these potential coverages should be explored.

What Data is Stored Electronically?

One may not want to publicize the precise types of information they maintain, but it is important to have an off-line inventory of the types of information for various reasons. For example, much information may not be particularly sensitive, and therefore possibly requires less protection than other types of information that may be more sensitive. Similarly, employees may have personal documents unrelated to a firm's "mission." A firm may have financial documents that are distinct from case files. Different types of documents may be treated differently. An inventory will help to determine this.

"Legacy" Data

This refers to traditional records. It is unlikely that this information can be inappropriately disclosed for obvious reasons. However, we minimize even these records by ensuring that client files are not visible to the people who visit our office.

Planned Data Destruction

Is there data that should be destroyed and, if so, what is that data and when should it be destroyed? In the case of our firm and many of our clients, there is a substantial amount of data, that can and must be destroyed pursuant to HIPAA. For example, individualized health care information, e.g., medical records, must be destroyed within a reasonable time after their use is no longer necessary. This "end-point" is likely to be several months after cases are settled and payments made when it is unlikely that settlements will be attacked.

While some entities have to maintain e-mails for prolonged periods, many e-mails (e.g., scheduling, reminders that are moot), do not need to be maintained. While there seems to be unlimited amounts of space to save data that is utterly unnecessary, it makes sense to not "keep" unnecessary data in perpetuity.

Each business needs to address when information can, should and/or must be destroyed according to the rules, regulations, customs and best practices of its industry.

Staff Devoted to Data Protection

The need for data protection has created many new work roles and employment opportunities, including privacy officers, information officers, technology officers, security officers, and their respective staffs. Small firms lack these resources which is yet another reason to maximize resources like policies and procedures to address what is a potentially complicated and costly process.

About the Rosenblum Newfield Law Firm

Founded in 1992, Rosenblum Newfield, LLC is a law practice with offices in New York and Connecticut. It has established a record of accomplishment based on its core values and on proprietary methodologies that have proven successful for its clients.

The firm concentrates in the defense side of civil litigation matters (with a special focus in medical liability cases/malpractice claims), administrative hearings and health care law. It is known for highly informed representation of medical professionals, nursing homes, home health care companies, and businesses in a variety of other industries. It maintains relationships with liability insurers throughout the United States, based on an appreciation of the business and financial pressures these companies face, as well as their reporting and procedural needs.

Its model is to remain a small firm of experienced lawyers. Each client receives the individual attention of senior attorneys.

The firm has earned the highest level (AV) in Martindale-Hubbell® Peer Ratings™ for its ethical standards and legal ability and is a member of the National Board of Legal Specialty Certification.

NYC: (212) 888-8001 • White Plains: (914) 686-6100 • Connecticut: (203) 358-9200