



Privacy and Security Incident Response Plan

Purpose

Tochtech Technologies is committed to appropriately protecting all information relating to its members and affiliates, as well as protecting its confidential business information (including information relating to its employees, affiliates, and members). To achieve this goal and to minimize the risk of loss, theft, or compromise of business or patient-related information, appropriate systems, operating procedures, and policies are in effect and are regularly reviewed and updated.

The purpose of this Privacy and Security Incident Response Standard Operating Procedure (SOP) is to provide a well-defined and organized approach for handling actual or potential threats to Tochtech's business or patient information maintained electronically (on computers and/or networks), or maintained physically in any other format. This SOP is intended to be durable, living document that may be amended in order to improve or clarify response processes.

The plan also identifies and describes the roles and responsibilities of the Privacy/Security Incident Response Team who will put the plan into action.

Scope

This response plan is meant to address privacy/security incidents involving any and all Tochtech data, including Tochtech data under the control or responsibility of a Business Associate or other third party.

Goals of Incident Response

In the event of a privacy/security incident, the goals of Tochtech's Privacy/ Incident Response Team are to:

1. Investigate the incident internally (in cooperation with law enforcement if necessary);
2. Mitigate potential harm to affected parties;
3. Minimize adverse impact to Tochtech in an ethically and legally appropriate manner, to include minimizing reduction in operations, reputational harm, and/or financial harm;
4. Appropriately communicate the incident or loss:
 - a. To affected parties in a timely manner (as appropriate or as otherwise may be required by law);
 - b. To regulatory agencies, news media, or other entities (as appropriate or required)
 - c. To staff (as appropriate or required, especially to leadership);
5. Provide guidance or assistance in the development of specific corrective actions (including disciplinary actions when appropriate); and

6. Conduct post-incident reviews, training and education, and provide internal communications in order to minimize potential future incidents.

Defining a Privacy/Security Incident

While the major goals described above are common to all privacy or security incidents, every privacy or security incident involves different degrees of potential risk and different potential for magnitude of harm to Tochtech. For instance, a minor incident may involve a low risk but inappropriate verbal disclosure of information that is non-sensitive in nature, while a major incident may involve loss or disclosure of sensitive information of multiple affected parties.

For the purposes of this response plan, a privacy incident is any attempt at, or occurrence of, unauthorized acquisition, exposure, disclosure, use, modification or destruction of sensitive data that compromises the security, confidentiality, or integrity of:

- Tochtech confidential business information (including information relating to its employees, and agents); or
- Individually identifiable information maintained by Tochtech, its affiliated entities or their agents;
- And:
 - May violate privacy/security regulations or laws; or
 - May result in the acquirer or another person taking some specific action with the information, (i.e. identify theft, extortion, sale of information, internet posting, reporting to media, etc.).

A Security Incident is any known or suspected event or condition which may put the confidentiality, integrity, or available of sensitive data at risk.

Incident Response Team Members

Appropriate members of the Incident Response Team will be determined by the nature of the incident, but may include a representative(s) from any/all of the following:

- Compliance Officer
- Security Officer
- Privacy and Security Analyst
- Legal Department
- Tochtech Senior Leaders
- Risk Management
- Information Technology Department

- Public Relations/Marketing Department
- Third party vendors engaged to provide incident response services

Incident Timeline

Incidents have a timeline that generally contains an Initial Response phase and a Continuing Response phase. Initial Response begins as soon as an incident is discovered or reported and includes time-sensitive first response actions to limit damage while a more organized response is being planned. Continuing Response includes all activities that are conducted necessary to close an incident case and include investigation, correcting processes, notifying affected individuals, and reporting to regulatory agencies as required by law. Generally, the activities within each phase are ongoing and may occur simultaneously, and there may be some overlap between Immediate Response activities and Continuing Response Activities. For instance, Investigation may uncover the need for additional Analysis, Containment, Communication, and activation of additional members of the Incident Response Team.

Discovery/Reporting

- Determination that an incident has happened
- Involvement of Area Management
- Involvement of IT Department
- Involvement of Compliance Department

Immediate Response (0--1 Business Day)

- Containment
- Opening of Incident Case Files
- Escalation
- Activation of the Incident Response Team and/or Alternate Plans

Continuing Response (0-15+ days)

- Analysis and Planning
- Investigation
- Mitigation and Correction
- Notification
- Closing of Incident Case File
- Reporting

Discovery or Reporting of a Privacy/Security Incident

Information relating to privacy/security incidents may be reported or discovered in numerous ways. Some of them are listed below.

1. Patients/members, family members, members of the general public, and others may report (or complain of) a privacy/security incident to any member of the Tochtech workforce to include employees and contractors, to include call center agents.
2. Employees may report an incident to local management.
3. Workforce members may submit a report by email (Outlook) using their @tochtech.com email address.
4. Employees may report Security Incidents by submitting IT tickets or by contacting staff in the Information Technology Department.
5. Employees may report directly to the Compliance Department in person, by email, or by phone to any member of the Compliance Department or by using the specified department email address (compliance@tochtech.com).
6. The Compliance function may observe an incident (for instance, while a member is conducting a staff training or during walkthroughs designed to detect risks or spot improper use, disclosure, storage, transmittal, or disposal of information).
7. Business Associates and/or Third Party Vendors may notify a department with whom they conduct business, a member of senior or executive management, or the Compliance Department.
8. Employees may call the Tochtech Compliance Hotline at 1-800-360-1286.

Incidents that should be reported may include but are not be limited to:

- a. Patient Privacy Complaints relating to:
 - i. Patient Privacy Rights
 - ii. Communications
 - iii. Inappropriate use, access or disclosure of health information
- b. Employee-related Privacy Concerns relating to:
 - i. Inappropriate use, access or disclosure of health information
 - ii. Inappropriate use, access or disclosure of confidential (non-health) information
 - iii. Inappropriate modification, deletion or destruction of health information
- c. Other Concerns relating to:
 - i. Loss or deletion of stored data; loss or theft of laptops, handheld devices, portable media storage containing confidential business or individually identifiable information.

- d. Theft or Loss of Tochtech Computer Equipment, including:
 - i. Desktop computers,
 - ii. Laptop computers,
 - iii. External hard drives
 - iv. Compact disks/DVDs
 - v. Blackberries/Tablets/PDAs,
 - vi. Thumb drives,
 - vii. Medical equipment that stores patient information, or
 - viii. Any other device or storage media (whether issued by Tochtech or not) which may contain business records or personal information of any potential compromise of Tochtech patients, staff or affiliates;
- e. Computer/Network Intrusions, Data Losses, or other Compromises, including:
 - i. The unauthorized access, viewing, copying, forwarding, or removal of electronically stored data; or
 - ii. Any other incidents that result/may result in unauthorized acquisition or release of any potential compromise of electronically stored business or patient information.
- f. Data Transmission Incidents, including:
 - i. Inadvertent e-mail releases
 - ii. Unsecured data transmission

Determining that an Incident has occurred

The Compliance Officer and/or designee(s) have final determination as to whether an incident has occurred that requires an incident response according to this Incident Response Plan. An incident is defined in the section titled “Defining a Privacy/Security Incident.”

If a determination is made that no incident has occurred, responding staff will take appropriate steps to close the response and document the non-incident facts and finding that no incident occurred. This may include communications to staff, keeping in mind that some findings may be restricted.

Involving Management and/or the IT/Compliance Departments

Upon discovery of an incident or receipt of a report that an incident has occurred by any member of the Tochtech workforce:

1. The receiving or discovering workforce member will perform initial information gathering regarding the incident to report to assist with response activities. In general, workforce members should gather:
 - a. The name and contact information of the reporting individual (if applicable)
 - b. The location of the incident

- c. The circumstances of the incident to include involved parties
2. The receiving or discovering workforce member will communicate incident information to area management, to the Information Technology Departments, and/or to the Compliance Department as appropriate to the circumstances by phone, email, Hotline, or other means.
3. If area management receives a report, it will immediately notify the Information Technology Department and/or the Compliance Department as appropriate to the circumstances.
4. Area management will communicate with the Information Technology Department and/or the Compliance Department (as appropriate to the circumstances) regarding actions to contain an incident, investigate an incident, and mitigate damage to affected individuals and to Tochtech.
5. The Information Technology Department and the Compliance Department will communicate and collaborate regarding privacy/security incidents.
6. Compliance may require the completion of an Incident Reporting form to obtain enough information to facilitate response.

Timeline Note: Timeliness in reporting to the Compliance Department is critical to ensure timeframes are compliant with law. By law, privacy/security breaches are considered “discovered” when any member of Tochtech’s workforce knows of it or *should* have known of it in the exercise of due diligence. This discovery date starts the clock that requires investigation and notification within specified timeframes.

For instance:

- A patient calls and leaves a voicemail with a complaint that indicates a breach has occurred. The voicemail is not checked for 9 days. The date of discovery is that date the voicemail was left, shortening investigation and notification timeframes by 9 days.
- A breach is reported to a manager on January 1. The manager loses the paper on his desk and comes across it on March 16. The date of discovery is January 1. According to law, the organization would already be past legally mandated timeframes and in violation of HIPAA’s Breach Notification Rule.

After Hours Emergencies

Generally, most incidents do not require an immediate response and employees can typically wait until the next business day to report. Employees are expected to use professional judgment to determine whether a known or suspected incident is severe enough to warrant an immediate urgent response. In such cases, the employee should contact the following in this order until able to reach one of the persons listed:

1. Security Official: 1-800-360-1286
2. Compliance Officer: 1-800-360-1286
3. Chief Information Officer: 1-800-360-1286

Initial Response

Tochtech's initial response to an incident can make the difference between a situation that is handled properly and a catastrophe. For instance, if a Security Incident is discovered involving hacking of a Tochtech system or network, the immediate steps taken to stop unauthorized access and secure data could make a huge difference in the amount of damage that could be inflicted to individuals and to Tochtech.

Depending on the nature of an incident, its scale, potential impact, risk to the organization, or other factors, Tochtech staff may respond in a variety of ways to include:

- Containment
- Opening of Incident Case Files
- Analysis and Planning
- Escalation & Activation of the Incident Response Team

Containment

When a breach is discovered, the Incident Response Team may determine the need to conduct containment activities to stop additional information from being lost or disclosed, or to reduce the number of persons to whom information may reach. Incident Response Teams members may, over their areas of responsibility or collaboratively, take steps to attempt having lost/stolen/inappropriately disclosed information returned or destroyed. For instance, area managers may attempt to contain and control an incident by suspending certain activities or locking and securing areas of record storage; Human Resources may suspend employees as appropriate to prevent compromising behavior; and the Information Technology Department may shut down particular applications or third party connections, reconfigure firewalls, change computer access codes, or change physical access codes.

The Help Desk must still be notified of the incident to insure proper notification, resolution and follow up by the appropriate members of the Incident Response Team.

If applicable, staff members closest to the incident will determine the extent of the incident by identifying all information (and systems) affected, and take action to stop the exposure. This may include:

- Securing or disconnecting affected systems
- Securing affected records or documentation
- Halting affected business processes
- Pausing any processes that may rely on exposed information or that may have given rise to the incident (as necessary to prevent further use/exposure/etc)

This would most typically occur in instances of electronic system intrusion, exposed physical (e.g. medical) files or records or similar situations.

If the incident occurred at/by a third party, the Incident Response Team will determine if a legal contract and business associate agreement exist. The Compliance Officer and/or designee will work with the Legal Department and the department holding the contract/business associate agreement to review the contract terms and determine the next course of action.

Cyber-insurance and Breach Response Vendors

If an active cyber-insurance policy exists or the need is otherwise determined, the Incident Response Team may contact contracted third party vendors (cyber-insurance vendors, others) for breach response services and resources to include forensics, investigation and response consulting, notification and call center services, etc. Though recommended to occur as soon as possible after discovery, this can occur at any point as more information is obtained or the need is otherwise determined.

Documentation/Opening Incident Case Files

Compliance will document all actions taken regarding an incident to include all steps taken in accordance with this plan. Compliance will begin to establish this documentation as soon as possible, at which point the incident response will be considered an open case file.

Generally speaking, documentation, at a minimum, needs to provide thorough, complete documentation of an incident that can be used to fulfill reporting requirements to government agencies and to organizational senior leadership, as well as serve as legal documentation in the case of a future legal or regulatory proceeding. This documentation will include notations of analyses, notification, reporting, communication, meetings, and all other actions. All documentation related to privacy/security incidents must be maintained and kept confidential according to the HIPAA Document Retention Policy.

Escalation/Activation of the Incident Response Team and/or Alternate Plans

As more information is gathered, responsible staff will assess each privacy/security incident to determine appropriate handling. This may involve the development and use of internal procedures by individual departments. For instance, while a minor and low risk incident may be assigned to and investigated by competent technicians within a department, the department may require that technician to escalate to management any incident that may damage the organization. The manager, in turn, may escalate the incident to the director, VP, or other level.

This may also involve activating alternate plans – for instance, the Disaster Recovery/Business Continuity Plans as appropriate.

Additionally, responsible departments will assess each privacy/security incident to determine which parties should be included in communications. For instance, the Compliance Department may grant view access to cases to responsible management to include area managers, directors, and vice-presidents unless circumstances exist that would preclude sharing information – for instance, if a conflict of interest exists, if sharing this information could compromise an investigation, or if the responsible manager (or a friend or family member of the responsible manager) is involved as an affected party, as a subject, or in other ways.


Some factors to consider when deciding whether to escalate:

1. Can the incident cause harm to an individual? To what degree?
2. Will the incident require reporting to affected parties, senior management, or government agencies?
3. Would the containment, investigation, correction, or other aspect of the incident benefit from cooperation between two or more departments?
4. Does the incident have the potential to cause financial or reputational harm, disruption of operations, or other adverse consequence to the organization?
5. Have involved parties (for example, a complainant) involved legal counsel or threatened legal action?
6. Does the incident involve a business associate or third party vendor?

Once analysis determines the need for escalation, the Compliance Officer will activate the Incident Response Team to an extent appropriate to each incident. The Compliance Officer will provide an initial overview of the situation as it pertains to each Incident Response Team member’s area of responsibility. For instance, the Director may engage the Legal Department when necessary as legal concerns arise or when invoking Attorney-client may be appropriate. The Compliance Director will also identify which Incident Response Team members will play an active role in the investigation and communicate with them accordingly.

Escalation: as scale, risk or impact increases, involvement increases*

Involved Parties	Technician (IT team member, Privacy and Security Analyst), Management (Area Manager, etc.)	Department Management (Compliance Officer, Security Officer, IT Director, etc.), Incident Response Team	Department Management (Compliance Officer, Security Officer, IT Director, etc.), Incident Response Team, Senior/Executive Management
------------------	---	---	--

	Low	Moderate	High
	Impact/Risk to Individuals/Organization Or Complexity/Scale 		

Responding workforce members are expected to use professional judgment in determining whether an incident is low, medium, or high on the spectrum of scale, risk, or impact. Generally speaking, a low priority incident is one which poses no risk to business operations and can be appropriately handled by a technician. A high priority incident poses clear risk to operations of all or part of the company, while medium priority incidents fall in between. When in doubt, responders should inform the Security Officer and/or Compliance Officer, who can then determine whether to include others in the incident response.

Continuing Response

Tochtech must continue to take action on a breach in order to understand what has happened, to reduce potential for damages resulting (both to affected individuals and to the organization), to correct what happened, to prevent future recurrence, to inform parties as appropriate, and to fulfill requirements of law.

To do so, the following steps must be carried out in response to privacy/security incidents:

- Investigation
- Mitigation and Correction
- Notification
- Closing of Incident Case File
- Reporting

Analysis and Planning

Upon notification of a real or potential privacy/security incident, the Compliance Officer or designee will perform a preliminary analysis of the facts and assess the situation to determine the nature and extent of the incident. Such analysis may include contacting the individual who reported the problem.

Analysis will also include research into any potential legal concerns beyond the more familiar federal regulations.

The Compliance Officer or designee, with guidance as necessary from Incident Response team members, will establish a specific incident response plan to investigate the incident, mitigate the damages associated with the exposure or disclosure of personal information, and communicate as necessary with staff, law enforcement, the media, and others. Timeliness of establishing and carrying out the plan may be critical to the public's image of Tochtech. As needed, any/all members of the Incident Response Team may be involved in carrying out the activities of the Incident Response Plan. The plan will address the following:

- **Review of initial containment activities**
 - Communication regarding containment activities taken thus far
 - Assessing risks to information and systems
 - Determination of additional containment measures
 - Determination of the need to inform law enforcement (for instance, it may be appropriate to notify the FBI in cases of identity theft or hacking) [Approval from Legal is Required unless the workforce member determines a delay could result in harm to the company or to individuals internal or external to the company]

- **Investigation Planning**
 - Assignment of and coordination with Investigators
 - Evidence gathering planning
 - Interview planning

- **Communications/Public Relations Planning**
 - Assess how an incident and the response to it may affect Tochtech's reputation and public image.
 - Internal Communications
 - Determine the need to notify Administration at one, some or all Tochtech facilities
 - Determine the need to notify all current employees of the incident or employees of the affected facility or department only
 - Determine how employees will be notified (email, mail to home, mandatory staff meetings, etc.)
 - Determine who will communicate to the staff
 - Determine material content of the notification
 - External Communications
 - Determine the need for external communications to covered entity, media (press conference or press release if Covered Entity is required to notify the media), etc.
 - Determine who will represent Tochtech publicly
 - Determine the material content of the Press Conference and/or Press Release
 - Determine the need to post information regarding the incident to the Tochtech website

Investigation

Thorough investigation, and documentation of that investigation, is a critical component of incident response. Thorough investigation and documentation needs to be timely, accurate, and professional, and serves several purposes as listed below.

Purposes of thorough Investigation:

- Shows due diligence in complying with legal and regulatory requirements.
- Provides management with accurate and detailed information. This is essential to correct processes, contain damage, communicate with staff and with external affected persons, and take other appropriate measures.

- Promotes fair, just, and more objective outcomes in regard to the handling of workforce members, especially as it pertains to discipline.
- Reduces the chances for mistakes that may occur due to incomplete or incorrect information.
- Provides documentation showing the organization's commitment to protection of the information it holds.
- Provides documentation that may be used in civil or criminal proceedings even years after an incident occurred.

Investigation needs to be timely to insure the most accurate information and to comply with required timeframes. Even so, internal investigations and gathering of data may take several days or even weeks. In the event that law enforcement is involved, this can stretch into months.

Investigation may involve:

- If lost/stolen equipment is recovered, the Information Services Department and the Security Officer may conduct detailed forensics on the equipment in an attempt to determine if business or personal information stored on the equipment was accessed or compromised in any way.
- Involved parties may need to notify local and/or federal law enforcement authorities to assist in further investigation, particularly in cases of lost/stolen equipment. In most cases, Legal and Risk Management should be consulted before law enforcement is contacted.
- If an incident involves a third party such as a business associate, staff may have to communicate with the third party determine which who will be responsible for notifying local and/or federal law enforcement authorities.
- The Human Resources Department may assist with interviewing workforce members; provide guidance to ensure consistent enforcement of discipline; and take action involving staff (such as suspending employees to prevent further damage).
- Complainants, recipients of inappropriately disclosed information, and others may be contacted for questioning or to request return or destruction of information.

Mitigation and Correction

Tochtech has a legal and ethical obligation to mitigate (reduce) any harmful effects that result from privacy and security incidents. Though this is only legally required if Tochtech "has actual knowledge of harm," Tochtech will also take reasonable and appropriate steps to prevent harm from occurring either to individuals or to the Tochtech organization. Actual privacy/security

incidents may result in negative outcomes for the affected parties several months or years later - Tochtech must acknowledge and be prepared to handle this risk appropriately.

Examples of Mitigation:

- Tochtech may provide “free” credit report monitoring and other “free” services that may be appropriate (such as credit counseling services or repeat medical testing) to affected individuals for specified period of time.
- Compliance, IT, and others may consult with Risk Management and Legal as necessary to understand full scope of risks and potential damages and ways to mitigate.
- Senior management may determine need for any legal action to be taken on parties (internal or external) involved in the incident.
- Responsible departments may determine need for termination of third party contract.
- Tochtech may contact third party insurers for services or resources related to any purchased policies (for instance, breach response services provided by a cyber-security policy).

Closely tied to mitigation, Correction should occur after any privacy or security incident in order to prevent future recurrence and to comply with organizational policy.

Examples of Correction:

- As appropriate, revise written policies and procedures that may be deficient.
- Assess informal/unwritten processes and practices and make changes that correct or improve them.
- Follow human resources policy and disciplinary action guidelines to determine need for disciplinary action on any Tochtech employee involved in the incident (Human Resources to be involved)
- Determine the need for additional staff training.
- Determine the need for increased security (physical or electronic) measures.

Notification

The Incident Response Team will determine what notifications are required and will make those notifications in a timely manner in accordance with federal law, state law, and organizational policy (for instance, the Tochtech Policy titled “HIPAA Breach Notification Policy” allocates the responsibility for notification of individuals affected by a privacy breach to its Privacy Official, who is typically the Compliance Officer). The Incident Response Team will:

- Determine the need to notify affected individuals. Both state and federal law may have requirements. Notifications should be timely, and conspicuous. Depending on the nature of the incident, notification information may be communicated to Affiliate Physicians, Business Associates, or others in order for those entities to provide notification.
- Determine if any other notifications to regulatory entities are required. For instance, specific states may require notification to the state Attorney General's office in the event a Social Security Number is breached.
- Determine if media notification is required (as required by HIPAA and Tochtech policy in some circumstances; composition and delivery of such notice will be conducted by or with approval of Public Relations).
- Determine the means by which individuals and/or other required parties will be notified. Notifications should be delivered in a manner that will ensure the individual receives it. Appropriate delivery methods include written letter, telephone call, or in some cases, substitute forms of notice (conspicuous posting on the website, notification to major media) as determined to be appropriate by the Compliance Department, in conjunction with the Legal Department
- Determine the material content of communication to affected individuals (portions may be pre-determined for efficiency)
- Communicate the incident to Affiliate Physicians/Covered Entities as required by law and contract.

Closing the Incident Case File

Before an incident case file can be closed, Tochtech must have met the goals of incident response. To recap, those goals are to:

1. Investigate the incident internally (in cooperation with law enforcement if necessary);
2. Mitigate potential harm to affected parties;
3. Minimize adverse impact to Tochtech in an ethically and legally appropriate manner, to include minimizing reduction in operations, reputational harm, and/or financial harm;
4. Appropriately communicate the incident or loss:
 - a. To affected parties in a timely manner (as appropriate or as otherwise may be required by law);
 - b. To regulatory agencies, news media, or other entities (as appropriate or required)
 - c. To staff (as appropriate or required);
5. Provide guidance or assistance in the development of specific corrective actions (including disciplinary actions when appropriate); and
6. Conduct post-incident reviews, training and education, and provide internal communications in order to minimize potential future incidents.

All information relating to the incident and activities to meet these goals will be documented in the incident case file before it can be closed. A closed incident case file will be retained according to the HIPAA Document Retention Policy.

Reporting

Tochtech will fulfill all reporting requirements under state and federal law. For instance, HIPAA requires notification to the Covered Entity within 60 days of a breach.

In the event that a breach involves more than 500 individuals, the Incident Response Team (Public Relations in particular) will prepare for fallout that may occur once the covered entity conducts notification of the media.

Additionally, for the purpose of organizational improvement, information from investigation case files may be used to report to staff and management of various levels in the form of trainings, reports, or other means. Identifying information (both of patients and of staff), patient specific information, and other sensitive information will be redacted as appropriate.