

ALLINA HOSPITALS & CLINICS
IDENTITY THEFT INVESTIGATION PROTOCOL CHECKLIST

I. Intake

- Each site must identify a Designated Lead - security lead at the facility OR, if there is no security lead, the facility manager or some other business unit leader - to receive the report and coordinate the review.
- Upon receipt of a report of identity theft, report the incident to the designated attorney within the Allina Legal Department.

II. Notification

- Convene an initial meeting of the Identity Theft Task Force.
- Review the alleged incident and discuss strategies for investigation and communication.
- Designate a Primary Investigator (in consultation with Allina Legal).
- Inform local law enforcement of the incident.
- Notify any other relevant internal resources.

III. Investigation

- Contact actual and potential victims to inform them that an investigation is underway.
- Advise victims of the need to contact police, credit reporting agencies, and organizations that may be impacted, and ask the victim to authorize those organization to release information to Allina for investigation purposes.
- Interview the victim to determine whether the individual has knowledge of inappropriate use of personal information or missing property.
- Contact law enforcement and organizations with whom the victim does business to obtain further information.
- Based on the information obtained, draft a list of potential suspects.
- Work with internal resources to obtain further information about potential suspects.
- Based on the information obtained, develop a limited suspect list.
- Conduct criminal history background checks on all suspects on the limited suspect list.
- Interview each individual on the limited suspect list, keeping in mind that the employee may need to be informed of the right to have a third party present.
- Determine primary suspect(s).
- Interview all primary suspects.
- If a suspect confesses, obtain a signed confession and immediately contact law enforcement.
- If the suspect does not confess, contact local law enforcement and provide all relevant information.

IV. Information Management

- Convene a meeting of the Task Force.
- Develop a plan to identify and communicate with all actual and potential victims.
- Meet with Media Relations to ensure appropriate communications to all parties, including the media.

V. Conclusion

- Schedule a final meeting of the Task Force to ensure appropriate documentation and communications processes were followed.

ALLINA HOSPITALS & CLINICS IDENTITY THEFT INVESTIGATION PROTOCOL

SCOPE AND PURPOSE

The purpose of this protocol is to provide guidance to business units within Allina Hospitals & Clinics (“Allina”) as to the proper processes for conducting an investigation of alleged or confirmed identity theft. This protocol is designed to guide the relevant parties within the affected business unit through the processes of intake, notification, investigation, information management, and investigation conclusion.

DEFINITIONS

Designated Lead: Individual designated by the site – generally the security officer or facility manager – as the intake person to receive and review reports of identity theft. The Designated Lead will convene the task force and coordinate the review of the incident.

Primary Investigator: An individual or individuals with primary responsibility for conducting an internal investigation of identity theft. At some sites (e.g. sites with Security Officers) the same person might be the Designated Lead and the Primary Investigator.

DNT Call Accounting System: An electronic system that tracks and generates reports on all outgoing calls from several Allina facilities.

Identity theft: Identity theft occurs when an individual “steals” the name, social security number, or other personal information of another to conduct fraudulent activities.

Identity Theft Task Force (Task Force): A group of individuals designated by the affected business unit to oversee the investigation of an alleged or confirmed incident or incidents of identity theft. The Task Force shall be comprised of at least one individual from the following areas: facility security (where applicable), business unit leadership, legal, media relations, risk management, human resources, information services, and compliance.

INVESTIGATION PROTOCOL

Intake

- A. The intake process is initiated when an individual contacts the facility to report an incident of identity theft. The party receiving this information must communicate the information to the security lead at the facility. If there is no on-site security lead, the information must be reported to a “Designated Lead.” The business unit leader may delegate responsibility for follow-up to another individual within the business unit, if the delegate has experience in dealing with security concerns.
- B. The Designated Lead must report the incident to the designated attorney within the Allina Legal Department. This Allina Legal Representative (ALR) is responsible for working with the designated lead to coordinate the investigation and provide advice regarding notification.

Notification

- A. Upon notification of an incident of identity theft, the Designated Lead, in consultation with the ALR, will convene an Identity Theft Task Force (“Task Force”). The Task Force shall be comprised of at least one individual from the following areas:
- Facility Security (where applicable);
 - Business Unit Leadership;
 - Legal;
 - Media Relations;
 - Risk Management;
 - Human Resources (“HR”);
 - Information Services (“IS”) Security; and
 - Compliance.
- B. The Task Force will review the alleged incident and discuss strategies for investigation and communication of the alleged incident.
- C. The Task Force will designate an individual or individuals with primary responsibility for conducting an internal investigation (“Primary Investigator”).
- D. The Primary Investigator will inform local law enforcement of the incident and prepare to conduct an internal investigation. The Primary Investigator will inform law enforcement that he/she will share all pertinent information obtained through the internal investigation, subject to limitations imposed by law and Allina policies.¹
- E. The Designated Lead and Primary Investigator, in consultation with the ALR, have primary responsibility for notifying all relevant parties of the reported incident. For notification purposes, relevant parties may include: law enforcement, confirmed and potential identity theft victims, impacted staff members, business unit leaders, business unit board members, human resources staff, and the media.

Investigation

A. General

1. Once local law enforcement has been apprised of an alleged incident of identity theft within an Allina facility, Allina will conduct a parallel, internal investigation of the alleged incident. The information obtained through this internal investigation will be shared with local law enforcement to the extent permitted by law. The Primary Investigator will keep the Designated Lead at the site informed as to the status of the investigation.

B. Collecting information

1. If the alleged victim or victims are patients, the Primary Investigator will contact the victim(s) to advise them that Allina is conducting an investigation into the incident. In order to facilitate the investigation, every patient must be informed that there are several steps the patient should take to mitigate the potential harm resulting from the incident. Specifically, the patient should be advised to:
 - a. File an official police report with the law enforcement department in the jurisdiction in which the incident occurred. Once a police report number is obtained by the patient, instruct the patient to provide this information to the Primary Investigator.
 - b. Contact one or all of the national credit reporting agencies and request that a fraud alert be placed on his or her credit report. A fraud alert will ensure that no one will be able to obtain credit in the victim’s name absent authorization from the victim.

¹ For specific information about Allina’s privacy policies, visit http://akn/corp_compliance/privacy_policies.html or call the Corporate Compliance Department, 612-775-5868.

- c. Contact any organizations (credit card companies, cellular telephone companies, etc.) that may have been used by the identity thief to conduct fraudulent transactions. Ask the patient to provide these companies with his or her permission to release information to Allina during the investigation. In order to obtain this information, the patient may need to sign a release form. This form can be obtained by contacting the ALR.
2. The Primary Investigator will also interview the patient and/or his or her family member(s) to determine:
 - a. whether the patient is missing any personal property (e.g., a wallet, purse, social security cards, credit card); and
 - b. whether the patient has any information as to the nature of the access to their personal information and the names of any individuals who may have had such access.
3. Once a police report number is obtained from the patient and the patient has provided permission for the Primary Investigator to contact credit card and other organizations on the patient's behalf, the Primary Investigator will contact the corporate fraud department within the relevant organization(s). The Primary Investigator is responsible for working with these organizations to obtain as much information as possible about the nature of any fraudulent transactions, including:
 - a. names, dates, addresses, phone numbers, and other identifying information on any credit or service applications;
 - b. the date of receipt of the fraudulent application or information; and
 - c. any surveillance images or signed receipts indicating or confirming the identity of the perpetrator.
4. Based on the information obtained from the victim(s), law enforcement, and any credit or service organizations, the Primary Investigator will determine the following:
 - a. the location or location(s) of the incident;
 - b. the nature of the information access (e.g., computerized records, discarded items, patient charts);
 - c. the names of facilities, departments, and individuals (including contractors, temporary staff, and agency staff) who had access to sensitive patient information when the incident occurred. These names and access information can be obtained by contacting IS Security, who can access the appropriate information systems, including staff schedules.
5. Based on the information collected, the Primary Investigator should be able to establish a list of potential suspects. The potential suspect list may be extensive and include current employees, former employees, associates of employees, temporary and agency staff, and visitors to the facility.

C. Investigation of potential suspects

1. Once a list of potential suspects is developed, the Primary Investigator will coordinate with several internal departments to obtain further information about the potential suspects.
2. If a potential suspect is a current or former employee, the Primary Investigator will contact the facility's HR department to obtain biographical information about the individual. This information should include:
 - a. the individual's current and previous addresses;
 - b. the individual's previous places of employment; and
 - c. the results of any background checks conducted in any jurisdiction where the individual has lived or worked.
 - d. The information obtained from HR must be compared to any information received from credit or service organizations involved in the incident to determine if there is a match. It is important to note that an individual who inappropriately accessed or "took" the patient information may not be the individual who actually "used" the information.

3. The Primary Investigator must also contact IS Security to obtain access to a number of information systems. Specifically, the Primary Investigator should:
 - a. request access to the facility's electronic list of all employees to determine whether the names of any employees match the names supplied by credit or service agencies involved in the incident; and
 - b. request that IS Security review all relevant patient record-keeping systems to determine who may have accessed the patient's information, when and where such access occurred and, if possible, why the information was accessed.
4. The Primary Investigator should also contact IS Telecommunications and request a review of the DNT call accounting system, if possible. If credit or service organizations involved in the incident provided a telephone number of the individual who engaged in fraudulent activity, it may be possible to determine whether anyone in the facility contacted the individual. If the call was placed from a telephone with limited access, the Primary Investigator should determine who has access to the telephone line, place those individuals on the potential suspect list, and investigate those individuals using the procedures listed above for all potential suspects.

D. Establishing a limited suspect list

1. Based on the information gathered on a potential suspect, the Primary Investigator will develop a profile of the suspect. Any employees on the potential suspect list that do not fit the profile should be removed from the list; those who do fit the profile will be placed on a limited suspect list.
2. The Primary Investigator will conduct criminal history background checks on all individuals on the limited suspect list. This background check should include searches in all local areas in which the suspect has lived or worked. The Primary Investigator should conduct background checks in close consultation with law enforcement.
3. The Primary Investigator will also conduct an interview of each individual on the limited suspect list.² The Primary Investigator will interview the individual and assess, through verbal and non-verbal behavior, whether the individual is providing information truthfully, or acting deceptively. Even if the interviewee is not the individual who fraudulently used the information of another, he or she may know or be associated with the perpetrator.
 - a. *Note:* All union employees have the right to request the presence of a union representative during the interview. The Primary Investigator need not inform the employee of this right unless the Primary Investigator intends to make an accusation against the individual. All non-union employees have the right to request the presence of any third party during the interview; they do not need to be apprised of this right.

E. Identifying and investigating the primary suspect

1. Following interviews with individuals on the limited suspect list, the Primary Investigator will narrow the list of suspects to one or more primary suspects. If the Primary Investigator is unable to identify a primary suspect or suspects, the Primary Investigator will resume interviews of individuals on the limited suspect list to obtain further information.
2. The Primary Investigator will conduct interviews of all primary suspects.
3. In the event that a suspect confesses to involvement in identity theft, the Primary Investigator will attempt to elicit as many details as possible, including the number of victims, the nature and location of the information access, and the ways in which the victim's information was used or distributed.
 - a. If possible, the Primary Investigator should get the primary suspect(s) to sign a written statement verifying the suspect's involvement in the incident.

² For specific information on proper interviewing techniques, please call the ALR.

- b. The Primary Investigator should immediately contact law enforcement and inform them of the confession so that the suspect may be turned over to law enforcement for further questioning and arrest. While awaiting the arrival of law enforcement, the Primary Investigator may detain the suspect for a reasonable amount of time (one hour maximum).
4. If the suspect does not provide a confession and does not cooperate during the interview, the Primary Investigator will contact law enforcement and provide all relevant evidence to them for further investigation. The Primary Investigator will also contact HR to discuss the suspect's employment status.

Information Management

A. Task Force meeting

1. Once a primary suspect is identified and all relevant information is provided to law enforcement sources, the designated lead will convene a meeting of the Task Force to apprise Task Force members of the status of the incident and discuss communications strategies.
2. The Task Force will review the information provided by the Primary Investigator and develop a plan to identify all actual and potential victims, and other parties impacted by the incident.
3. The Designated Lead, in consultation with the ALR, a Media Relations representative and the Primary Investigator, will work with the designated lead to establish appropriate communications tools and timeframes for communicating to all relevant parties, including: actual and potential victims, staff on the affected unit(s), HR, business unit and organizational leadership, board members, and the media. Any communications with the media must be conducted in consultation with business unit leadership.

Investigation Conclusion

- A. The Designated Lead will schedule a final meeting of the Task Force to ensure that all appropriate processes have been documented and resolution of the matter has been clearly communicated to all necessary parties.