

Appendix 1: Identity Theft Red Flags Mitigation and Resolution Procedures

Identity Theft Red Flags	Prevention/Mitigation Procedure	Resolution of Red Flag
Suspicious Personal Identifying Information		
Documents provided for identification appear to have been altered or forged. The photo or physical description of the person is not consistent with the appearance of the person.	Stop the application/billing process and require person to provide additional satisfactory documentation to verify identity.	Original documentation must be provided to resolve discrepancy and continue the admissions/ billing process. Notify law enforcement as appropriate
Personal identifying information provided by the person is not consistent with other personal identifying information provided.	Stop the application/billing process and require person to provide additional satisfactory documentation to verify identity.	Original documentation must be provided to resolve discrepancy and continue the admissions/ billing process. Notify law enforcement as appropriate
Personal identifying information provided is of a type associated with fraud. For example: the address is fictitious; phone number is invalid or associated with a pager	Stop the application/billing process and require person to provide additional satisfactory documentation to verify identity.	Original documentation must be provided to resolve discrepancy and continue the admissions/ billing process. Notify law enforcement as appropriate
The SSN provided is the same as that submitted by other persons opening an account or other customers	Stop the application/billing process and require person to provide additional satisfactory documentation to verify identity.	Original documentation must be provided to resolve discrepancy and continue the admissions/ billing process.
Personal identifying information provided is not consistent with personnel information that is on file with the financial institution, creditor or VMH	Stop the admission/billing process and require person to provide additional satisfactory documentation to verify identity.	Additional documentation must be provided to resolve discrepancy and continue the admissions/ billing process. Notify law enforcement as appropriate
Resident has an insurance number but never produces an insurance card or other physical documentation of insurance	Stop the admission/billing process and require person to provide additional satisfactory documentation to verify identity.	Additional documentation must be provided to resolve discrepancy and continue the admissions/ billing process.

Appendix 1: Identity Theft Red Flags Mitigation and Resolution Procedures

Identity Theft Red Flags	Prevention/Mitigation Procedure	Resolution of Red Flag
Suspicious Account Activity		
Information about unauthorized charges in the resident's account	<p>Stop all account activities</p> <p>Notify the resident and/or NOK to provide additional satisfactory documentation to verify account activity.</p>	<p>Begin an internal inquiry into the account activities.</p> <p>Notify law enforcement as appropriate</p>
Mail sent to the resident's home that's returned repeatedly as undeliverable although transactions continue to be conducted in connection with the resident's covered account	<p>Stop all account activities.</p> <p>Skip-tracing procedures are used to find the resident's current HOR address</p>	<p>Resident's family/responsible other notified</p> <p>Notify law enforcement as appropriate</p> <p>If the results of the investigation do not indicate fraud, all contact and identity information is re-verified with the resident</p>
Notice From Other Sources		
<p>A complaint or inquiry is received from a resident based on receipt of:</p> <ul style="list-style-type: none"> -a bill for another person; -a bill for a product or service the resident denies receiving; -a bill from a healthcare provider that the resident never patronized; -a notice of insurance benefits (or explanation of benefits – EOB) for health services never received by the resident; -information added to a credit report by a healthcare provider or insurance company; -a collection notice from a bill collector with whom the resident has had no transactions. 	<ul style="list-style-type: none"> -Investigate the complaint; -Interview individuals as appropriate; -Contact the other healthcare provider or insurance company; -Gather as much information as possible concerning the questionable bill. 	<p>Contact the resident's family or POA to discuss the situation;</p> <p>Inform the CEO/designee of this discrepancy;</p> <p>Contact the local or State police, as needed, to notify them of these suspicious circumstances</p> <p>Follow police instructions, or contact the State Division of Consumer Affairs.</p>

Appendix 1: Identity Theft Red Flags Mitigation and Resolution Procedures

Identity Theft Red Flags	Prevention/Mitigation Procedure	Resolution of Red Flag
<p>VMH is notified by a resident who is a victim of identity theft, by law enforcement, or by others that it has opened a fraudulent account for a person engaged in identity theft.</p>	<p>Investigate to determine if account was opened fraudulently or if billing was made fraudulently.</p>	<p>Contact the CEO/designee</p> <p>Additional documentation must be provided to resolve discrepancy and continue service process. Contact insurance company as necessary</p> <p>Notify law enforcement as appropriate</p>
<p>An employee or volunteer or agency worker has access to a resident's SS number and other identifying information and buys goods based on resident's ID.</p>	<p>Investigate the complaint; Interview individuals; Gather as much information as possible concerning the theft of a resident's identity.</p>	<p>Contact CEO/designee and the local or State police.</p> <p>Contact the credit card company, cancel that account number</p>
<p>Resident or insurance company report that coverage for legitimate hospital stay is denied because insurance benefits have been deleted or a lifetime cap has been reached</p>	<p>Investigate complaint, interview individuals as appropriate</p>	<p>Additional documentation must be provided to resolve discrepancy and continue service process. Contact insurance company as necessary</p> <p>Notify law enforcement as appropriate</p> <p>If the results of the investigation do not indicate fraud, all contact and identity information is re-verified with the resident</p>
<p>Evidence that Resident Account files were accessed by unauthorized person(s)</p>	<p>Investigate complaint/incident, interview individuals as appropriate</p> <p>If determination is made which files were accessed; re-verify account with resident or resident responsible party.</p> <p>Take disciplinary/legal actions as required</p>	<p>Enforce policy that Resident Account files must be locked when not in use.</p> <p>Limit access to files</p> <p>Provide dual lock security (i.e. door, file cabinet)</p> <p>Conduct periodic random review of Resident Accounts</p>
<p>Evidence that Resident Medical Records were accessed by unauthorized person(s)</p>	<p>Investigate complaint/incident, interview individuals as appropriate</p> <p>Take disciplinary/legal actions as required</p>	<p>Maintain accurate/timely records sign-out log</p> <p>Process enforced to initial for key and use, log reviewed by Nursing supervisor</p> <p>Records locked when not in use</p>

Appendix 1: Identity Theft Red Flags Mitigation and Resolution Procedures

Identity Theft Red Flags	Prevention/Mitigation Procedure	Resolution of Red Flag
Complaint by a resident or observant employee that mail has been tampered with	Investigate complaint/incident, interview individuals as appropriate Take disciplinary/legal actions as required	One department will be designated to handle all mail (i.e. Social Services) This entity will then distribute both resident and VMH mail to appropriate addressee
Complaint or observation by employee that Resident Face Sheet was being used/read by unauthorized individual(s)	Investigate complaint/incident, interview individuals as appropriate Take disciplinary/legal actions as required	Report observation of unauthorized personnel accessing Face Sheet Report and missing face Sheets Educate staff on need to safeguard face Sheets
Complaint or observation by employee that Resident “Blue Card” was being used/read by unauthorized individual(s)	Investigate complaint/incident, interview individuals as appropriate Take disciplinary/legal actions as required	Lock “Blue Cards” in box with limited access to keys/place box in a more concealed location Destroy current “Blue cards” replace with cards that contain to resident critical information Train staff on sensitivity of “Blue Cards” and requirements to safeguard information contained on them
Complaint or observation by employee that unauthorized access to electronic data especially MDS, has occurred	Investigate how unauthorized access occurred, interview individuals as appropriate Take disciplinary/legal actions as required	Passwords changes every 90 days Employees instructed to log off computers when not in use and turn off at the end of the work day Instruct employees not to write down pass words and leave them in proximity to their computer; remove/block access points All incident recorded in security Officer’s Log
Complaint or observation by employee that unauthorized access to Medical Insurance files has occurred/files containing identity records found open	Investigate complaint/incident, interview individuals as appropriate Take disciplinary/legal actions as required	All Medical Insurance files locked at when not in use Establish dual lock security (i.e. door and file cabinet) If determination made which files were observed, VMH will re-verify account with appropriate insurance company

Appendix 1: Identity Theft Red Flags Mitigation and Resolution Procedures

Identity Theft Red Flags	Prevention/Mitigation Procedure	Resolution of Red Flag
Complaint or observation by employees that unauthorized access to employee records, payroll records, health records has occurred/files found open	Investigate complaint/incident, interview individuals as appropriate Take disciplinary/legal actions as required	All employee records/ files locked when not in use Establish dual lock security (i.e. door and file cabinet) If determination made which files were observed, VMH will re-verify contents

Revised: January 2011
Revised: August 2013