# Table of Red Flags – Detection and Mitigation Steps

<table>
<thead>
<tr>
<th>Red Flag Detected During VUMC Process</th>
<th>Trigger Event for Identity Verification Alert (ID Alert)</th>
<th>Immediate Response</th>
<th>Mitigation Steps (Follow links to steps Defined on pages 5-8)</th>
</tr>
</thead>
</table>
| Suspicious documents presented by the patient or guarantor at the time registration or the visit | Drivers license or insurance card (or other documents) presented appear to have been altered | • Copy or scan the document presented;  
• enter the ID Alert indicator;  
• make note in the comments section of Medipac or Epic about why the alert has been set;  
• continue registration without challenging the patient; and then,  
• notify supervisor, as soon as possible, after patient is processed | Immediate: [Steps 1 - 5];  
Supervisor: [Steps 6 - 7] |
| | Picture or physical description provided on drivers license or other ID document obviously does not appear to match the person presenting | • Copy or scan the document presented;  
• enter the ID Alert indicator;  
• request a second piece of ID and if provided also copy or scan; continue registration;  
• make notes in the comments section of Medipac or Epic about why the alert has been set;  
• continue the registration without challenging the patient; and then,  
• notify supervisor, as soon as possible, after patient is processed | Immediate: [Steps 1 - 5];  
Supervisor: [Steps 6 - 7] |
| Suspicious or conflicting identification or clinical information recognized | SSN provided by presenting patient is already on file associated with another name and/or same name but a different date of birth | • Confirm that the SSN given was entered correctly;  
• If registration is in person, verify identification by requesting two forms of ID to include:  
  ✓ Government issued photo ID, such as driver’s license; and,  
  ✓ SSN card or  
  ✓ Birth certificate or | Immediate: [Steps 1 - 5];  
Supervisor: [Steps 6] |
### Table of Red Flags – Detection and Mitigation Steps

<table>
<thead>
<tr>
<th>Red Flag Detected During VUMC Process</th>
<th>Trigger Event for Identity Verification Alert (ID Alert)</th>
<th>Immediate Response</th>
<th>Mitigation Steps (Follow links to steps Defined on pages 5-8)</th>
</tr>
</thead>
<tbody>
<tr>
<td>In the clinical care setting</td>
<td>Information documented in the medical record is inconsistent with the information provided by the individual presenting for care (e.g. physical characteristics or medical/family history)</td>
<td>✓ Marriage license or ✓ Divorce degree or ✓ Municipal tax or utility bill showing name and address. • Copy or scan the documents provided; • If this SSN problem presents during a telephone registration (e.g. call centers), then scheduler or call center person asks the patient to bring the Social Security Card along with the insurance card at the time of the visit; • leave the SSN blank on the account being registered, but capture the number given at registration in the notes; (Epic will leave the SSN blank, Medipac will generate a SSN that is the CPI number) • make a note in the comments section of the account record for the SSN given (in case there is further issue of identity theft); • enter the ID Alert indicator on both records; • make note in the comments section of Medipac or Epic on each record about why the alert has been set; • continue registration without challenging the patient; and then, • notify supervisor after patient is processed</td>
<td>Immediate: [Steps 1 – 5]; Supervisor: [Steps 6 – 7]</td>
</tr>
</tbody>
</table>

Last update: 30April09
### Table of Red Flags – Detection and Mitigation Steps

<table>
<thead>
<tr>
<th>Red Flag Detected During VUMC Process</th>
<th>Trigger Event for Identity Verification Alert (ID Alert)</th>
<th>Immediate Response</th>
<th>Mitigation Steps (Follow links to steps Defined on pages 5-8)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ED Clinical staff “recognizes” having cared for this person previously under a different name</td>
<td>ED Clinical staff “recognizes” having cared for this person previously under a different name</td>
<td>• Notify the ED registration supervisor&lt;br&gt;• ED registration sets the ID Alert and notes reason for the alert in the comments section of Medipac</td>
<td>Supervisor: <strong>Steps 6 – 7</strong></td>
</tr>
<tr>
<td>Alerts or notices received from external agencies or service providers</td>
<td>Notice from insurance company, TennCare, or insurance fraud investigator about identity theft or suspicious activity or fraud.</td>
<td>▪ Identify VUMC accounts/records impacted;&lt;br&gt;▪ Set the ID Alert indicator;&lt;br&gt;▪ Enter note in the comment section of Medipac and/or Epic about reason for alert;&lt;br&gt;▪ Supervisor notifies MIS and/or the Privacy Office</td>
<td><strong>Steps: 8 – 12</strong></td>
</tr>
<tr>
<td>In Patient Accounting: billing and collections</td>
<td>Identity Verification Alert (ID Alert) is already attached to this patient’s record from previous information</td>
<td>▪ Refer to the notes present in the comments section of Medipac or Epic to understand why the alert has been set;&lt;br&gt;▪ Explain to patient that there are notes on the account instructing them to confirm ID by requesting to see and copy the document(s);&lt;br&gt;▪ Copy or scan the documents presented;&lt;br&gt;▪ Leave the alert in place;&lt;br&gt;▪ Update the notes in the comments section;&lt;br&gt;▪ Continue registration;&lt;br&gt;▪ Notify Supervisor immediately upon completion of the registration process.</td>
<td>Immediate: <strong>Steps 1-5</strong>, except notify supervisor immediately&lt;br&gt;Supervisor: <strong>Steps 6-7</strong>&lt;br&gt;Supervisor may escalate VPD contact</td>
</tr>
<tr>
<td>At the time of registration for admission or a visit</td>
<td>Security Risk Indicator – ID Theft (IDT) is already attached to this patient’s record from previous information</td>
<td>▪ Refer to the notes present in the comments section of Medipac or Epic to understand why the alert has been set;&lt;br&gt;▪ Explain to patient that there are notes on the account instructing them to</td>
<td>Immediate: <strong>Steps 1-5</strong>,&lt;br&gt;Supervisor: <strong>Steps 6-7A</strong></td>
</tr>
</tbody>
</table>

---

**Last update: 30 April 09**
Table of Red Flags – Detection and Mitigation Steps

<table>
<thead>
<tr>
<th>Red Flag Detected During VUMC Process</th>
<th>Trigger Event for Identity Verification Alert (ID Alert)</th>
<th>Immediate Response</th>
<th>Mitigation Steps (Follow links to steps Defined on pages 5-8)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notice from Patients, Victims, Law Enforcement Authorities, or Others Regarding Possible Identity Theft</td>
<td>Patient receives billing statement, an EOB from insurance company, or collection notice for services not received or a provider the patient never saw</td>
<td>confirm ID by requesting to see and copy the document(s); ▪ Copy or scan the documents presented; ▪ If government issued photo ID is NOT presented or does not appear to be the patient, immediately notify a supervisor who may escalate to contact VPD as deemed appropriate by department protocol; ▪ Leave the alert in place; ▪ Update the notes in the comments section; ▪ Continue registration.</td>
<td></td>
</tr>
<tr>
<td>Patient or other victim reported</td>
<td>Patient proactively reports they have been the victim of identity theft to prevent future occurrence at VUMC</td>
<td>Notify Patient Accounting who will identify accounts and review current billings to confirm accuracy ▪ If no billing error is apparent, Patient Accounting will notify the Privacy Office to initiate internal review</td>
<td>Immediate: Steps 1 – 5 Supervisor: Step 12 Privacy Office: Step 13 Team: Steps 14 – 16 Privacy Office: Step 17</td>
</tr>
<tr>
<td>Law Enforcement or other external agency reported</td>
<td>A victim of identity theft has initiated legal, law enforcement or credit recovery action that may involve VUMC accounts</td>
<td>Notify Patient Accounting who will identify accounts and review current billings ▪ Notify Privacy Office who will confirm police report and initiate the Security Risk Indicator for Identity Theft (IDT)</td>
<td>Immediate: Steps 8 – 12 Privacy Office: Step 13 Team: Steps 14 – 16 Privacy Office: Step 17</td>
</tr>
</tbody>
</table>

Last update: 30April09
# Table of Red Flags – Detection and Mitigation Steps

## Response and Mitigation Steps at the Point of Registration or Service:

### Immediate Response by the Registrar/Receptionist/Pt Accounting Rep:

- **Step #1A:** If the individual is physically present, collect and scan/copy additional forms of identification, if available:
  - Government issued photo ID,
  - SSN card,
  - Birth certificate,
  - Marriage license,
  - Divorce degree, or
  - Municipal tax or utility bill showing name and address

- **Step #1B:** If the individual is on the phone, instruct him/her to bring in the Photo ID, SSN Card, and Insurance Card at the time of the visit;

- **Step #2:** Set the Identity Verification Alert (ID Alert)

- **Step #3:** Make note(s) in the comments section of Medipac or Epic about why the ID Alert has been triggered

- **Step #4:** Continue the work operation without challenging the patient

- **Step #5:** Notify a supervisor, as soon as possible, after processing the patient

### Mitigation Steps by the Supervisor:

- **Step #6:** Review details of situation including the notes in Medipac and/or Epic to verify accuracy and determine escalation path

  - **Step #7 A:** Supervisor **confirms** suspected identity theft or fraudulent documents:
    - Updates notes in the comments section of Medipac and/or Epic
    - Leaves in place the “ID Alert”
    - Supervisor may report incident to VPD for support in investigating the incident.

  - **Step #7 B:** Supervisor **resolves** the issues initially identified above by finding error or confirming identity:
    - Updates notes in the comments section of Medipac and/or Epic
    - Removes the “ID Alert”

  - **Step #7 C:** Supervisor **is not able to confirm or resolve** the identification questions:
    - Updates the notes in the comments section of Medipac and/or Epic
    - Leaves the “ID Alert” in place
Table of Red Flags – Detection and Mitigation Steps

**Early Response and Mitigation Steps upon Receipt of Notice of Suspected or Actual Insurance or Medical Fraud:**

**Mitigation Steps by Patient Accounting:**

Step #8: Identify any accounts associated with this individual at VUMC (hospital or professional services)

Step #9: Set the “ID Alert” in the patient’s accounts in Medipac and Epic;

Step #10: Make notes in the comment section of both Medical and Epic about why the “ID Alert” has been triggered

Step #11: Refer the case for review by Ass’t Director of Patient Representatives or designated supervisor in Patient Accounting

**Early Response and Mitigation Steps upon Receipt of Notice or Claim by Patient of Identity Theft:**

Step #12: All reported incidents/claims of identity theft from patients or other external sources are referred first to the billing areas (via the Assistant Director of Patient Representatives) for review of the charges by date of service to determine whether or not a billing error has occurred.

- When a billing error is found, the billing area contacts Medical Information Services to have the medical record(s) involved reviewed for accuracy and corrected, if applicable.
- When patient accounting manager rules out billing error, the incident/complaint is referred to the Privacy Office to be evaluated as a possible case of identity theft and the bills associated with the account(s) involved are put on HOLD pending further review and determination.

Step #13: The Privacy Office attempts to substantiate the claim of identity theft by reviewing the VUMC documentation together with the information provided by the person initiating the claim/complain (the “alleged victim”).

- The alleged victim is asked to complete a Police Report. Each claim of identity theft associated with medical fraud is reported to the VPD as soon as possible after it is discovered.
- VPD investigates, as needed, and completes a fraud report when the identity theft is alleged to have occurred at VMC.
- The alleged victim is required to provide a copy of the identity theft police report if filed with another police jurisdiction.
- The services and dates of service documented in the medical record are reviewed with the alleged victim to identify whether the alleged victim has ever been a patient at VMC.
- The Admitting Manager is contacted to set the “ID Alert” on the record/accounts and place a note in the comments section of Medipac and/or Epic.
Response and Mitigation Steps for Cases with Unresolved Identification Verification Alerts:

Step #14: A report is produced daily for the admitting/registration supervisors identify any new ID Alert indicators set the previous day. In addition, a report is generated periodically (likely monthly) identifying every medical record that has continues to have an active “ID Alert”.

Step #15: An ID Alert Review Team meets as needed (likely monthly) to review the ID Alert cases to determine next steps for responding to the circumstances that precipitated setting the ID Alert.

Step #16 A: Based upon the collective information available, the team may recommend that the ID Alert be removed from a record because the issue has been resolved or is believed to have been a processing error.

Step #16 B: If the team continues to believe that there is reason to question the identification information on file, then the ID Alert will remain in place with a note in the comment sections of both Medipac and Epic to positively confirm identification of this person at the next visit or encounter.

Step #16 C: If sufficient information has been secured to confirm a case of identity theft:

- Admitting will set the Security Risk Indicator: IDT for confirmed (or probable) case of identity theft.
- Patient Accounting and the VMG Business Office adjust the billing information so that the alleged victim is not charged for the services provided to the perpetrator. Final disposition of the claim for services rendered to the perpetrator may be kept in a HOLD status until further external criminal fraud investigation is completed. Patient Accounting notifies the affected insurance carriers or payors about the affected account(s).
- Medical Information Services determines whether the medical record impacted contains information about more than one individual.
  - If the record contains only clinical information about the perpetrator of the identity theft, then MIS removes the “victim’s” identification information from the electronic and paper records and replaces the name on the record with “John Doe-Identity Theft” and the notes the Privacy Office incident tracking number in the address field.
  - If the medical record contains clinical information associated with the real patient AND the perpetrator of the identity theft, then MIS creates a new “John Doe-Identity Theft” record and moves the clinical information from the dates of service associated with the identity theft to the John Doe record. The clinical information relating to the John Doe is deleted from the real patient’s medical record.
  - If, or when, the real identity of the perpetrator is confirmed, the name associated with the John Doe medical record for that individual is changed to the real name of this patient.
- VPD determines and processes any additional criminal law enforcement steps that may need to be taken.
- The Office of General Counsel determines if any additional fraud reporting is required.
Table of Red Flags – Detection and Mitigation Steps

Step #16 D: If a claim of patient identity theft is not considered valid because the alleged victim is not willing to file a police report or other official report of medical fraud and/or the driver’s license photo and/or signature on file appear to match the identity and signature of the alleged victim:

- Patient Accounting and the VMG Business Office process the claim(s) for payment for services rendered using the patient and guarantor information collected at the time of registration.
- Medical Information Services makes no change to the medical record for this patient.

Step #17: The Privacy Office notifies the alleged victim regarding the VMC determination and next steps:

- If the claim of identity theft is found valid: advise the alleged victim of the steps taken to address the identity theft, including:
  - Setting the Security Risk Indicator – IDT for Identity Theft and the need for the patient to always present government issued photo ID at the point of service;
  - Explain the steps taken to correct the medical record information;
  - And explain the steps taken to correct the billing information.
- If the claim of identity theft has been sufficiently substantiated, explain that no further action will be taken at VUMC without additional information to substantiate the claim.