

## Mitigation Considerations for Potential Inappropriate PHI Disclosure

- A) Determine what actually occurred.
1. Was this a policy violation?
  2. Not currently defined in a policy but should be?
- B) Breach?
- Yes: Could it have been prevented?
- Policy issue?
  - Process issue?
  - Technical Issue? Contact Vendor?
  - People issue? Education needed? Disciplinary action needed?
- No: Does additional education or re-education need to occur?
- Staff?
  - Patient?
- C) What exactly is the PHI that was disclosed?
- Medical information
  - Financial information
  - Unknown
- D) How did the disclosure occur?
- Lost? Original or copy?
  - Verbal?
  - Written document?
  - Misdirected FAX?
  - Email?
  - Hacker?
- E) Who received the breached PHI?
- Internal
  - External
    - Covered entity?
    - Public entity (news media, company, other)?
    - Private citizen?
    - Government source?
    - Unknown?
- F) Based upon the answers above, determine and analyze the potential risks to the patient.
1. Possible identity theft?
  2. Is patient a VIP such that medical information is potentially news worthy?
  3. Was PHI relative to HIV status, substance abuse, mental health, STD?
- G) Determine appropriate actions:
- 1) Notify legal?
  - 2) Notify risk management?
  - 3) Notify public relations?
  - 4) Notify the patient?
- Determine urgency
- Locate contact information and patient preference: phone call, certified letter
- If identity theft concerns exist advise patient to:
- File a police report and send copies to banks and credit card companies
  - Contact Federal Trade Commission: 1-877-IDTHEFT (1-877-438-4338)
  - Fill out a Federal Trade Commission complaint form
  - Notify their local post office that identity theft occurred because mail fraud is often a part of the crime
  - Inform the SSA if their social security number was fraudulently used

- Contact the IRS If they encountered a tax violation as a result
- Review their credit report with the three main credit bureaus: Equifax, Experian, and Trans Union
- Have the credit bureaus put out a fraud alert
- Inform check verification companies if checks or checking accounts were involved
- Notify fraud or credit departments at credit organizations
- Document all contacts with the above parties.

5) Requires process change?

6) Requires policy revision?

7) Requires technical intervention?

*Internal, External?*

8) Accounting for disclosures log?

9) Notification needed? (FBI, OIG, FTC, CMS, state agencies, other?)

H) Determine person/position responsible for actions

I) Follow-up to assure actions required have been carried out.

J) Document entire process and outcome.

Contact Information:

[http://consumer.gov/idtheft/con\\_steps.htm](http://consumer.gov/idtheft/con_steps.htm)

[https://rn.ftc.gov/pls/dod/widtpubl\\$.startup?Z\\_ORG\\_CODE=PU03](https://rn.ftc.gov/pls/dod/widtpubl$.startup?Z_ORG_CODE=PU03) (FTC ID Theft Complaint Form)

Equifax: 1-877-576-5734; [www.equifax.com](http://www.equifax.com)

Experian: 1-888-397-3742; [www.experian.com/fraud](http://www.experian.com/fraud)

TransUnion: 1-800-680-7289; [www.transunion.com](http://www.transunion.com)

Equifax

P.O. Box 740256

Atlanta, Georgia 30374

Experian

P.O. Box 9532

Allen, Texas 75013

TransUnion

P.O. Box 6790

Fullerton, CA 92834