Indian Health Service

HIPAA & Privacy Investigation – From start to finish

HEATHER H MCCLANE, MBA

SENIOR OFFICIAL FOR PRIVACY / PRIVACY OFFICER

23 AUG 2023

Purpose

The Privacy investigation process is an organized approach to making determinations as to whether a breach or violation has occurred.

Conducting internal investigations is one of the most important steps to establishing whether violation of the law has occurred.

An organized framework can be helpful during an investigation to help provide consistency and ensure objectivity.

The administrative requirements of HIPAA Privacy Rule 164.530 requires a process for individuals to make complaints and then requires documentation of those complaints and their disposition—essentially requiring an investigation.

Develop your framework

Written Complaint

Incident Risk Assessment

Conflict of Interest

Policies & Procedures

Security Parameters – Electronic and Paper

Establish Previous Training

Formulating Investigative Questions

Fact Finding

Due Process

Making Sanction Recommendations

Investigative Reports

Retention

Written Complaint

Before an investigation can be completed, we must receive a complaint in writing. Be sure this is a true complaint and not something like “see who was in my records”.

Alternately, we conduct our monthly monitoring of all staff access, including area office staff, under §164.308(D). If you as HIM Directors see suspicious activity, we can file an F07-02b form here: https://hqabqdispswhd01.d1.na.ihs.gov/helpdesk/WebObjects/Helpdesk.woa/wo/3.7.21.1 and our filing of the IRF serves as a written complaint.

Retain this complaint or the SPT report with your investigative file

Incident Response

Every reported privacy and/or security incident warrants immediate attention and a full investigation to determine whether a breach has taken place.

It is critical that the determination is made accurately and in a timely manner so the appropriate actions can be taken—such as applying sanctions or following breach notification requirements.

Reminder - Covered entities have 60 days from the date of discovery to ensure compliance with all breach notification requirements.

A reported incident can be a violation, a breach, or neither. The process and investigation for determining a breach must be highly detailed, thorough, accurate, and completely documented.

It must capture all elements of the incident such as date of incident, type of Protected Health Information (PHI) involved, details of what happened, and any person(s) involved.

Examples of Incidents

Lost Personal Identity Verification (PIV) Card

Lost computer

Unattended Personal Identity Verification (PIV) Card

Lost Government Cell Phones

Unauthorized Access

Unauthorized Disclosure

Unattended Computer

Sending email containing Protected Health Information (PHI) via Outlook

Documents containing Protected Health Information (PHI) left on a printer or fax machine or copier

Incident Risk Assessment

It is essential to conduct the HIPAA required incident risk assessment for every identified incident where Protected Health Information (PHI) is involved.

This means we examine and document the nature and extent of the Protected Health Information (PHI) involved, including the types of identifiers and the likelihood of re-identification;

Whether the Protected Health Information (PHI) was rendered unreadable;

The unauthorized person who used the Protected Health Information (PHI) or to whom the disclosure was made;

Whether the Protected Health Information (PHI) was actually acquired or viewed; and

The extent to which the risk to the Protected Health Information (PHI) has been mitigated.

Conflict of Interest

If the investigator has a possible conflict of interest, it is important that the investigator recuse themselves and ask another Privacy Liaison or Area Consultant to handle the investigation.

The recusal should be in writing and maintained with the investigation file.

Conflicts of Interest could be:

The accused is a family member, previous or current spouse (boyfriend/girlfriend)

Previous EEO activity with the accused

Friendships

Policies & Procedures

Review the facility policy for safeguarding Protected Health Information (PHI).

If this is unauthorized access to paper Protected Health Information (PHI), you may have to determine if the un-authorized access took place in the HIM department, if it did, you will need a copy of the HIM Department Access Policy.

Review the policy for access to Protected Health Information (PHI).

Review the policy for Minimum Necessary.

Review the disclosure policy of the facility.

Note – If you have previously reviewed the facility policies, you will simply verify with the facility that the policy is current or if it has been updated you will review the new policies.

Make sure you have a copy of the current year's Rules of Behavior

Security Parameters (Electronic)

Go into RPMS and ^spt or ^bdg (depending on how spt is set up at your service unit)

Go to USP, then option 3, print the list of DG security key holders

Go back to USP, option 1, print the screen that opens

You want to show that your security parameters are set to purge after 365 days, not before

You also want to show that all staff are blocked from accessing their own records.

Print this screen and retain with your investigative file

Important Reminder

As Chief HIMS key holders, even though your SPT is set to block you, you will still have access to your own record.

The same applies to Chief MIS key holders.

To fix this, you should ask your Area HIM consultant or IT Site Manager to go to the EAR option in SPT and enter restriction for you from your own chart.

You should then make sure that you go to EAR and enter restrictions for your IT staff as well.

Security Parameters (Paper)

Review the facility policy for safeguarding paper Protected Health Information (PHI).

If this is unauthorized access to paper Protected Health Information (PHI), you may have to determine if the un-authorized access took place in the HIM department, if it did, you will need a copy of the HIM Department Access Policy.

Review the policy for access to paper Protected Health Information (PHI).

This would include the disclosure policy of the facility.

Retain these policies with your investigative file

Establish Previous Training

This will include asking your Information System Security Officer (ISSO) for the employee's most recent Information Systems Security Awareness (ISSA) training date – You will want to accomplish this in writing and retain response with your investigative file.

Gather copies of training certificates or sign in sheets with training dates for the employee(s)

Retain this information in your investigative file

Formulating Investigative Questions

When you formulate your investigative questions, you want to be sure that you do not divulge Protected Health Information (PHI) of the complainant or subject of the investigation.

Keep it simple, example:

On July 1, 2015 at 18:36 you accessed the record of Demo, Parent; Under what authority did you access the record?

Or where multiple access exists:

On the following dates you accessed the record of Demo, Parent; Under what authority did you access the record?

Fact Finding

Leave space for the employee to type in their own responses

Give the employee enough time to answer the questions in writing, usually 3 to 4 business days

Make sure you have a statement such as: “Please be aware that you may be asked to answer further questions or provide further clarification of your responses”.

Be sure to include 18 USC 1001 just before employee signature line

Do not send these interview questions via Outlook instead use Secure Data Transfer

18 U.S.C. § 1001

I understand that Under 18 U.S.C. § 1001. Statements or entries generally (a) Except as otherwise provided in this section, whoever, in any matter within the jurisdiction of the executive, legislative, or judicial branch of the Government of the United States, knowingly and willfully— (1) falsifies, conceals, or covers up by any trick, scheme, or device a material fact; (2) makes any materially false, fictitious, or fraudulent statement or representation; or (3) makes or uses any false writing or document knowing the same to contain any materially false, fictitious, or fraudulent statement or entry; shall be fined under this title, imprisoned not more than 5 years.

Conducting Interviews

You can conduct face to face interviews as opposed to paper interviews.

However, keep in mind that a verbal interview has no record of question and response, aside from what each party may separately document.

This has the potential to lead to “he said, she said” situations.

If you choose to conduct face to face interviews, you will want to document the interview and ask the employee to sign your document indicating they agree with your version of events, keeping in mind, should the employee decline to sign you are back to “he said, she said”.

Reminder - union employees have the right to union representation during these interviews (they cannot answer the questions for the employee).

Due Process

Keep in mind that it is extremely important that we ensure that both the agency and the employee are treated fairly, with respect and dignity.

This means that we follow our policies and the law.

All of our incidents are actually reported to Office for Civil Rights (OCR) at the end of every calendar year.

Office for Civil Rights (OCR) can choose any of them in which to conduct a compliance review.

Investigative Reports

Once you've organized your notes and reviewed your evidence, you must draw a conclusion and make a recommendation. To keep it simple, it can take the form of:

The complaint is founded, with a brief explanation.

The complaint is unfounded, with a brief explanation.

The investigation is inconclusive, with a brief explanation.

Your conclusion and subsequent recommendation should rely on the facts, take into consideration any applicable laws and be fair and reasonable from both perspectives.

Investigative Reports (cont.)

An investigative report should be written and retained for each violation.

The report should include:

Date of reported incident or complaint received;

Incident Response Team (IRT)/Computer Security Incident Response Center (CSIRC) Numbers

(no investigation should be completed without a corresponding CSIRC) number)

The allegation;

The fact finding process;

Witness Interviews, if any;

Investigative questions and responses;

Dates of previous training;

Whether the complaint is substantiated or unsubstantiated with explanation of the findings;

Recommended sanctions, if any;

Any retraining required or completed

Making Sanction Recommendations

We are required to make sanction recommendations under the HIPAA regulations at 45 CFR §164.530.

Keep in mind that regardless of what we recommend, these are still federal employees who have rights and it is up to ER/LR and the employees supervisor to determine through Douglas Factors what the actual disciplinary action is, if any.

Simply request the ER/LR Track It ticket from the supervisor when you provide the investigative report so that you can close the Incident Response Team (IRT).

We will only request the actual sanction applied when warranted by an Office for Civil Rights (OCR) compliance review, Merit Systems Protection Board (MSPB) appeals etc. Otherwise, we have no need to know.

HIPAA Disposition Schedule

Under 45 CFR §164.530 we are required to maintain all records regarding HIPAA investigations, monitoring and such for six years.

The agency's disposition schedule provides for this and can be found here: http://www.archives.gov/records-mgmt/rcs/schedules/index.html?dir=/departments/department-of-health-and-human-services/rg-0513

Whistleblower Protection

Reporters of incidents to the Incident Response Team (IRT) are whistleblowers and their identities should be protected.

§160.316 Refraining from intimidation or retaliation.

A covered entity or business associate may not threaten, intimidate, coerce, harass, discriminate against, or take any other retaliatory action against any individual or other person for—

(a) Filing of a complaint under 45 CFR § 160.306;

(b) Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing under this part; or

(c) Opposing any act or practice made unlawful by this subchapter, provided the individual or person has a good faith belief that the practice opposed is unlawful, and the manner of opposition is reasonable and does not involve a disclosure of protected health information in violation of subpart E of part 164 of this subchapter.

Things to consider

Level of knowledge. How much training and education does the staff member have with respect to patient privacy and security expectations? Has this individual completed new employee orientation (Information Systems Security Awareness (ISSA), HIPAA) that addresses patient privacy and security responsibilities? Has he or she received job-specific privacy and security education and enhanced training, if applicable?

Previous violation. Does the staff member have a history of previous violations? Does he or she have a record of similar privacy/security violations with application of corrective actions or sanctions?

Sanction history. Review your organization's sanction history to ensure that you are being consistent with respect to levels of discipline. What is your facilities history of corrective actions for similar occurrences?

Questions


INDIAN HEALTH SERVICE
PHS · 1955 ·