Conducting HIPAA/Privacy Act & 42 CFR Part 2 Investigations

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, when we conduct our monthly monitoring of all staff access, including area office staff, under §164.308.

Check USP Under SPT/BDG

- 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.

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.

Formulating Investigative Questions

- When you formulate your investigative questions, you want to be sure that you do not divulge 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?

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”.
- Do not send these interview questions via Outlook instead use Secure Data Transfer (if you have a D1)

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 letter of the law.
- All of our incidents are actually reported to OCR at the end of every calendar year.
- OCR can choose any of them and conduct a compliance review.

Making Recommendations

- We are required to have a Sanctions Policy 45 CFR 164.530.

Incidents

- Lost PIV
- Lost computer
- Unattended PIV
- Unauthorized Access
- Unauthorized Disclosure
- Unattended Computer
- Sending email containing PHI via Outlook unencrypted
- Documents containing PHI left on a printer or fax machine or copier