Information Systems Activity Review

Sample triggers for review of protected health information (PHI) access

- Patient complaints
- Employees accessing other employees’ accounts
- Employees with concerns or suspicions of inappropriate access
- Failed login attempts
- Incidents or events that are high-risk (possible abuse, medication types, local outbreaks, etc.)
- Unusual patterns of login activity
- Sensitive diagnoses (social diseases, pregnancy, mental health, etc.)
- Employees accessing accounts after their work hours
- Employees who have the same last name, address or street name as the patient (accessing family records)
- Employee logins used after their termination
- High-profile or well-known, VIP patients (politicians, other providers, celebrities, local well-known individuals etc.)
- Random audits
- Newsworthy patients (incidents that might appear in the newspaper: wreck, industry accident, homicide, infant death, etc.)
- Employees who have remote access — need to monitor their use and activity
- Patient accounts being accessed when they were not treated recently or had no activity on their account for a period of time
- Business associate or contractor use of logins and access
- Employees viewing patient accounts they are not working on or patients they are not assigned (nurses on specific units, billers assigned to process specific insurance, lab tech access outside their need-to-know, etc.)
- Billers viewing insurance categories they do not process

PROCEDURE: This sample list was developed to assist facilities to promote continual awareness of any information system activity that could suggest a security incident. Not all reviews are required to be completed. Organizations can pick and choose types of reviews based on activities specific to their practice.

REPORT CONSIDERATIONS: Depending on the type of request, consider time frame and frequency when determining type and amount of information to be audited. Start with a small sample size (suggest starting with 30 records) or small period of time (suggest looking at first week of each month or every other Friday). If issues are found, add time frames or additional records to the audit. The finding may trigger an incident review — follow the incident and breach notification procedure policy.

Some event types will lend themselves to auditing specific dates or specific applications within your EHR or other software that maintains PHI (lab, practice management, medications, etc.). Consider asking the EHR vendor if the software has the capability to lock down specific patient accounts or methods to limit access or disclosure to patient accounts.

Lists generated can be saved electronically and do not have to be printed. Written/typed documentation explaining reviews, results and any follow-up actions should be kept for six years.