Audits of Systems and User Activity

The following selected reviews will be performed on a routine basis. The reports will be reviewed for any indication of inappropriate activity by a user or an unauthorized individual or program. The type of review will determine its frequency.

Audit Type	Frequency	Responsible Party/Report Provided By:
Activity in EHR/PM or any other system with PHI		
☐ Number of attempted or failed logons or lockouts by user-ID		
☐ Date of last password change by user-ID		
☐ Activity report for excessive/repetitive access to certain record(s) o Can be by VIP records or by user-ID		
☐ New/edited/deleted records by user-ID		
☐ Excessive data exports/reports, printing, or faxing o Can be system/software-wide or by user-ID		
☐ Access outside of work hours by user-ID		
Network and email activity		
☐ Remote access by user-ID		
☐ Unauthorized file access o Can be by VIP records, record location on network, or by user-ID		
☐ Number of attempted or failed logons or lockouts by user-ID		
☐ Date of last password change by user-ID		
☐ Hard drive/desktop audit for ePHI by machine		
☐ Access outside of work hours by user-ID		
Administrative processes		
☐ Appropriate user access or role permissions for network and all software with PHI		
☐ Processed patient access requests		

Audit Type	Frequency	Responsible Party/Report Provided By:
☐ New employee onboarding (how was access to PHI determined/granted)		
☐ Employee offboarding (was all access removed, was it removed quickly)		
☐ BYOD Inventory (are devices authorized, do any need removed)		
☐ Transport logs for all PHI that leaves the office (paper or electronic)		
☐ Business Associate (non-employee) access by user-ID o how many of a BA's employees have elevated or admin access to systems/software? o how/where can they access?		
☐		
☐		

Reports and audit logs will be retained for 6 years in a restricted file.

These are examples of questions to consider when creating or requesting a report from your IT Support or software vendor. Some reports may be automated. Keep them in mind when you see a report or a summary, if provided. Not all are mandatory for every report but can be helpful to spot unauthorized activity.

- Who is the user?
- What did the user do? (log-in, export or print a lot of information, edit, delete, access VIP) See if a user is logging-in an excessive number of times – or if multiple users are being locked out of their accounts. That is a sign of a cyberattack.
- Where did it happen? (file/system/record name)
- Where was it from? (were they at the office or remotely accessing - if possible)
- Is it appropriate for their role? Are they involved in that patient's care? Is it their neighbor or friend?
- When did they do it? (date and time) Was it outside of work hours? Was it after they were no longer employed there?
- For software and network access reviews, compare each user's level of access to PHI and ability to edit, create, delete, or otherwise modify the system with:
  - Their role and responsibilities. Is it too much access or "power"?
  - How much do they actually use the access they have? In other words, do they really need the access? Think about the minimum necessary standard.
  - Are they a current employee? It is important to remember to disable all access and change passwords when an employee departs.

Download the *HIPAA Audit Log Tracking Tool* and and the May 2020 article about audit logs on the TMC Client Portal to help you schedule and organize your reviews.