ASHNHA ALASKA STATE HOSPITAL & NURSING HOME ASSOCIATION

ODHIN Content Sharing

ODHIN is a very powerful tool that contains a variety of data. You as a user are responsible for ensuring that any content you share from ODHIN according meets all HIPAA standards regarding use and disclosure of patient health information (45 CFR 164.502, 45 CFR 164.506), as well as the BAA signed by your hospital. Below are some reminders regarding what you can and cannot do when sharing ODHIN content internally and externally.

When sharing ODHIN content **internally:**

- If sharing Patient Identifiable Information, financial data, or quality data, ensure all audience members are authorized to view such data. Do their roles allow them to access the data being shared?
    - Follow the "minimum necessary" guideline from HIPAA and limit sensitive data to the minimum amount necessary for the intended recipient(s).
- Is there a way for the audience to retain the data? Will this presentation be recorded or print screens of ODHIN content be included in handouts?
    - If so, make sure to inform the audience of the HIPAA/BAA restrictions and that the material is only to be shared internally on a need-to-know basis.
- If the data being shared includes facility identifiers such as hospital name, only share aggregated data.
- Make sure that you prevent "accidental sharing" by protecting print-outs, locking screens, only downloading data to secure locations, etc.

Things to keep remember when sharing ODHIN content **externally:**

- If ODHIN content is being shared externally/publicly, or somewhere that is publicly discoverable, then the data must be fully deidentified per HIPAA standards and stripped of the following patient identifiers:
    - Patient or family names
    - All geographic subdivisions smaller than state
    - All elements of dates
    - Telephone numbers
    - Fax numbers
    - Email address
    - Social security number
    - Medical record number
    - Account numbers
    - Health plan Beneficiary
    - Certificate/license numbers
    - Vehicle identifiers
    - Device identifiers and serial numbers
    - URLs
    - IP addresses
    - Biometric identifiers
    - Full face photos
    - Any other unique identifying numbers
- Content that identifies individual hospitals cannot be shared externally.
- If your board meetings are public, share any non-deidentified data (such as analyses that identify hospitals or ZIP codes) during the non-discoverable executive session.
- If you would like to share an analysis or data that contains hospitals or PHI identifies, please contact us to review the request. If you receive requests from external sources, such as public health agencies, for data that would contain any of these identifiers (including hospital or county), please refer them to Elizabeth King or Jeannie Monk at ASHNHA so we can work with them to review and fulfill their data request appropriately.

Never share your log in credentials with another person. Doing so is a violation of the user agreement and will result in termination of access.