Mergers & Acquisitions:
Due Diligence in Corporate Compliance & Privacy Programs

NEHIA & HFMA December 2021

Patricia Ariel, NEHIA President, Retired(9/2021) SVP & Chief Compliance Officer
Westchester Medical Center Health Network

Agenda

- The M&A Team
- Due Diligence Set up
- Organizational Process
- Compliance & Privacy Review Plan
- Compliance Report to Diligence Team

The M&A Team

- Confidentiality
- Focused discussion in M&A Plan
- Listed Department Reviews
- Who will take overall lead
- Appoint those responsible for each review
- Risks

Due Diligence Set Up

- Attorney-client
- Confidential shared drive for the team
  - Same for the acquired organization
  - Identified confidential contacts
- Scheduled meetings for team
- Standard due diligence lists
  - Department specific questions for acquired organization
- Confidential communication and discussion on going with team
- Reporting upon information gathering

Organizational Process

- Data, data, data!
  - Using shared drive
  - Who will review gathered data?
- On site review
  - Is this possible?
  - Can an audit be performed?
- Interviews
  - Only with identified individuals

Compliance & Privacy Review Preparation

- Compile questionnaire
  - comprehensive
- Be prepared to discuss audit reviews done internally
- Ensure discussion with counsel and M&A team to make sure confidentiality is preserved and to stay within legal guidelines.

Compliance & Privacy Review- continued

Questionnaire examples:

- **Compliance Plan**:
  - Organizational Chart
  - 3 years board minutes
    - Written reports
  - Excluded provider reviews: reports? Any found in last 3 years? OIG/GSA/other
  - 3 years compliance certifications – Federal & State
  - Internal & external audit reports, gov't surveys, audits
  - Code of Conduct
  - How is annual education done? Completion rate?

Compliance & Privacy Reivew continued

Compliance Plan continued:

- Annual Risk Assessment & Work Plan
- Compliance Investigation Log, helpline cases
- Corrective Action Plans
- Policies

Auditing & Monitoring

- Are there auditing and monitoring activities on going? How?

Frequency? Reports to Boards?3-5 year look back.

Governmental Investigations

- Identify any OIG subpoenas, settlement agreements, voluntary and self disclosures,etc.

Compliance & Privacy Review continued

HIPAA Privacy & Security

- Documentation of complaints for privacy violations, HI-tech, etc.
- OCR complaints and CAPS
- Were there any on site OCR reviews
- Designated privacy & security officer
- Copies of written responses, if possible, redacted
- Breaches of business associate agreements
- Any third party reviews

Compliance Report to Diligence Team

- Conclusions
  - What did the data reveal?
  - Could you confirm statements or materials delivered by the acquiring organization?
  - Did you identify areas of risk? If so, what direction was taken to identify any financial or potential media risk?
  - Can you identify areas of weakness that could be addressed?
  - What were the strengths in the program?