The Provider Alliance
SHARING IDEAS, RESOURCES, AND PURPOSE

'HOT TOPICS' BRIEFING | 2018

COMPLIANCE WORKGROUP

SUMMARY

While there is rarely a 'slow' moment in the updates and news for human service providers, we do often see some themes emerge. For TPA compliance professionals, we wanted to provide a short briefing of some recent 'hot topics' and some tips for reducing risks and improving operational compliance.

TOPIC 1: Mobile Communication & Protecting Health Information

Text messaging has become nearly ubiquitous on mobile devices. According to one survey, approximately 72 percent of mobile phone users send text messages. In human services, we are not immune from the trend, and in fact many of our supervisors and direct care workers appear to embrace texting at work. It is essential for us as healthcare providers to understand the communication needs of our workforce in order to appropriately address any privacy and security risks they may pose. As many providers have discovered, trying to control how your workforce communicates is easier said than done, and policies and procedures often fail to account for direct service communication preferences.

Here are some general reminders as you work to manage mobile communications and secure protected health information for your organization:

- Generally, it is okay to send messages by text provided that the content of the message does not include "personal identifiers" and it's okay for a provider to send text messages to an individual or authorized representative, provided that the message complies with the "minimum necessary standard".

- Generally, it is also okay to send messages by text when the mechanisms are in place to comply with the technical safeguards of the HIPAA Security Rule; the technical safeguards of the HIPAA Security Rule are the most relevant for managing access controls, audit controls, integrity controls, methods for ID authentication, and transmission security mechanisms when health information is being transmitted electronically.

- Keep in mind, most standard "Short Message Service" (SMS) and "Instant Messages" (IM) often fail to meet the HIPAA Security Standards. Senders of SMS and IM text messages have no control over the final destination of their messages. They could be sent to the wrong number, forwarded by the intended recipient or intercepted while in transit. Copies of SMS and IM messages also remain on service providers´ servers indefinitely (and/or on the devices) exposing the organization to security and privacy vulnerabilities.

- Keep in mind that the fines for a breach of HIPAA can be considerable - a single breach of HIPAA can cost an organization up to $50,000 per day the vulnerability is not addressed (this includes employee behaviors).

So - What should you do?

- **Establish Clear Electronic Communication Standards**: make sure your policies and standards of conduct include expected behaviors for electronic communication.

- **Educate Employees**: make sure you train and remind everyone in your workforce of the expectations of privacy and confidentiality (especially with electronic communications).

- **<u>Evaluate Secure Solutions for Mobile Messaging</u>**: there are many secure solutions on the market for providers that encapsulate PHI within a private communications network that can only be accessed by authorized users. You can explore options to include secure messaging as part of an overall mobile device management solution.

TOPIC 2: Assuring Compliance for Defining Independent Contractors

The department of Labor and Internal Revenue Service have been targeting ongoing efforts to actively identify individuals who are misclassified as Independent Contractors. As employer accountabilities increase, Wage and Hour is aggressively auditing independent contractor relationships posing significant risk of costly audits, potential litigation, and even penalties for noncompliance or misclassifying relationships. As many providers struggle with maintaining a sufficient workforce, independent contracts may be a tempting alternative.

As compliance leaders, it's important that we help our human resource, program and financial colleagues understand potential 'red flags' in mitigating our risks for misclassification:

- Does the relationship with the individual last more than 12 months?
- Is the relationship recurring?
- Is the work performed formerly done by an employee?
- Is the prospective independent contractor a former employee? Are they doing a similar function?
- Is the work of the contractor integral to the organizations day to day operations?

So - What should you do?

- **<u>Review your Contracting Policy:</u>** make sure you have a contracting policy that clearly defines the terms and conditions of the independent contractor.

- **<u>Adopt Evaluation Tools:</u>** Establish a questionnaire to evaluate independent contractor relationships.

TOPIC 3: Investigating Allegations of Workplace Harassment

Since the social media hashtag #MeToo spread virally in October 2017, the near daily revelations of sexual harassment and assault across numerous industries call all of us as compliance professionals and employers to consider changes in our investigation and employment practices to promote safer and more inclusive workplaces for all employees.

The overarching question we face is this: When an employee makes a harassment complaint, is the organization ready to respond? Although most human service organizations have written policies prohibiting workplace harassment, we can experience challenges responding quickly when employees report harassment (e.g. deciphering the facts). Regardless of our good intentions to properly respond to complaints, poor planning and difficulties with the intake of the complaint, delays in initiating an investigation, failure to properly investigate or remediate the alleged harassment, inadequate communication with the parties, or some combination of these unforced errors can create substantial issues for us.

As compliance leaders, it's important to assure that our policies, procedures, and systems are in place and properly working to be able to effectively respond if and when allegations of workplace harassment and assault show up on your desk.

Here are some helpful tips:

- ✓ Make sure you review the standards of conduct with colleagues as part of your annual compliance training. Emphasize the importance of reporting all complaints of harassment to the compliance officer and/or HR.
- ✓ When you receive an allegation, make sure to identify an investigation lead and follow your policies for suspension.
- ✓ Be prompt in the investigation; initiate and conclude it with in a standard time frame (typically 5 days).
- ✓ Interview all potential witnesses and be sure to preserve documentation and evidence.
- ✓ Document the investigation using a standard format.
- ✓ Whether the allegation is founded or not, it's important to take steps to avoid retaliation on the work unit.
- ✓ Follow-up! Make sure to take action AFTER the investigation is completed and a determination has been made and be sure to keep the concerned parties informed of the progress and investigation activities
- ✓ MOST IMPORTANT - BE CONSISTENT!!

TOPIC 3: Electronic Visit Verification (UPDATE)

In late May 2018, the US Senate and House introduced bipartisan legislation (HR 5912 in the House and S 2897 in the Senate) designed to delay implementation of the Electronic Visit Verification (EVV) provision of the 21st Century Cures Act and require public input from stakeholders. The bill was led by Senators Lisa Murkowski (R-AK) and Sherrod Brown (D-OH) and co-sponsored by a range of Democrats and Republicans in the Senate and House

The EVV delay bill gives states an additional year to implement EVV, having it take effect on January 1, 2020 instead of January 1, 2019.

So – what should you do? Continue to focus on advocacy.

- ★ Based on recommendations from early adopter states, persons served and direct support workers expressed concern about having to learn and use multiple systems under a hybrid or provider choice model. This is a key consideration as our members work with the state in selecting solutions; many early adopter states indicate a statewide system is easier to navigate and this helps with trouble shooting and assuring accessibility.

- ★ Based on the experience of early adopter states, persons served and their families expressed concerns about the requirement that the location of services be electronically verified. TPA members should work with the state to select a solution that assures that HIPAA data privacy requirements would be maintained in the EVV system and that location would not be tracked for any other purpose than for verification of services. The EVV system should be accessible wherever services are provided (since personal care services can be provided at home or wherever normal life activities take an individual) and we believe TPA members should advocate for a state solution that includes 24/7 technical support with simple instructions and easy-to-use interfaces and processes that allow for persons served and their families to see and verify data before it is sent to the state for processing.

- ★ To minimize the provider burden, TPA members should have the ability to correct mistakes in EVV transactions.

- ★ Implementation of an EVV will inevitably have some cost implications for TPA members. It's important to advocate that such costs be minimized and be offset with benefits. If providers need staff to support or maintain the system, any added expense by TPA members must be reflected in rates for reimbursement. EVV as a system cannot be an unfunded mandate in Pennsylvania!

- ★ TPA is committed to working with ODP in support of selection of a solution to help them understand requirements that are not burdensome to large providers may be burdensome to some of our smaller provider members. ODP should not adopt a system that requires providers to add additional staff and offer a system that is available in multiple languages. The system should have an offline option for entering visit data and assure that it's easy to train and use to avoid further exacerbating the workforce crisis with direct service workers (e.g. driving direct support workers out of the workforce and worsen the current worker shortage).

- ★ TPA members should advocate for a system that is flexible in order to schedule services and accommodate multiple caregiving scenarios (e.g. direct support workers who live with individuals or shared care with one worker caring for multiple people at the same location)

- ★ TPA members should advocate for a system that is both accessible to individuals and their families to help maintain a person-centered approach and the system should seamlessly interface with current electronic medical record (EMR) systems.