VANREIN COMPLIANCE

Key Duties and Responsibilities of a Privacy and Compliance Officer

The Privacy and Compliance Officer will work in conjunction with multiple departments to fulfill these duties: IT, HR, Company Leadership, Legal, etc.

1 Implementation of Compliance Program

- Risk Assessment
- Research, understanding of federal & state regulations
- Creation of policies and procedure
- Training
- Documentation

2 Risk Management

- Ongoing, day to day upkeep of compliance (policies and procedures)
- Ongoing, day to day mitigation of identified risks
- Review of compliance program and implementation of the program
- Tracking and logging user access levels and user authentication
- Tracking and logging technology
- Managing physical security procedures and keeping logs of visitor access
- Managing risk management strategy and adjusting procedures as needed
- Keeping up to date with federal and state regulations to update policies as needed
- Managing ongoing employee training
- Ensuring Business Associate Agreements, Subcontractor Agreements, and NDAs are signed with appropriate vendors, clients, and other contractors.
- Documentation

3 Incident Response and Notification

Breach response
Breach notification (note: does your state have more stringent requirements?)
Emergency mode operations*
Business continuity*
Disaster response and recovery*

* related to mitigating risk and protecting PHI and ePHI in those circumstances

www.vanreincompliance.com
hello@vanreincompliance.com
830-201-1880

VANREIN COMPLIANCE

Incident Response & Disaster Recovery

Your Privacy Officer should be the point person implementing the Business Continuity and Disaster Response Plans – and they should be clearly laid out for everyone to follow.

Take some time to review the past year, write out what worked and what didn't (and plans to adjust for the future), and assess where there may have been vulnerabilities in your system. Here are a few questions to get you started.

1. Who is your point person if an incident or disaster occurs?_____
2. Do you have a plan to identify the risk and take steps to mitigate it? ☐ Yes ☐ No
3. What systems or applications do you need to have running to continue business operations? (If something happens, what's the minimum you need to keep running?)

4. What changes were made in the past year that worked and should be included in your policies and procedures for future disaster response?

5. In the event of a disaster, who are the key contacts that need to be reached? Do you have this list at hand for the relevant people?
   Ex. Are you tenants in your building? Do you call the landlord/property manager? Who is the point of contact for your IT company? Utilities/Phone/Internet?

6. In the event of a security incident or a breach, you need to: 1) Determine if it is a breach, 2) Conduct a risk assessment and determine what happened, 3) Send out relevant notifications in a timely manner depending on the scope of the breach, and 4) Document what occurred. Who in your company is responsible for, and will be involved in, each of these steps?

www.vanreincompliance.com
hello@vanreincompliance.com
830-201-1880