

Compliance Today – May 2020 Creating an effective open-door policy

By Solomon Carter

Solomon Carter (solomoncarter2000@gmail.com) leads the Office of Professional Development for the Physicians Group Practices, Patient Financial Services, at Emory Healthcare in Atlanta, GA. He also serves as a consultant specializing in compliance, professional development, and policy.

I'm a fan of open-door policies (ODPs) and believe that the concept can stunt risk and mitigate issues long before they metastasize.

But like all things, an ODP needs to have a robust policy behind it and be structured in a way that employees and management can benefit from it the most. If not, it can become anathema to your operational integrity.

Open-door policies can be much trickier than you think

When implementing an open-door policy, the first thing you should understand is that if you talk about it or teach it (which are the same thing), from that moment on, it becomes the formal policy of your organization. There's no such thing as an informal policy! I teach that the term "informal policy" is a serious threat to your risk matrix and should be mitigated enterprise-wide. If you have an open-door policy, make sure it's in writing.

The second thing you have to consider is how to protect the integrity of your organizational structure (your chain of command). An improperly administered policy can entice insubordination and cause dissention throughout the organization. It can also make managers feel marginalized and give unmerited employees a false sense of authority.

If you don't want to create an atmosphere of tattling, then there are several components that must go into a robust ODP that's functional, effective, and a strong resource for your staff.

Set the boundaries

Be succinct in what the policy is.

Here's a basic open-door policy template:

"An open-door policy is designed to bring an urgent or emergency matter to the attention of a manager or executive leader whose position is above that of, or lateral to, your immediate supervisor.

"An urgent or emergency matter includes, but is not limited to, the following:

- "A threat (or completed act) of physical violence from an employee;
- "A threat (or completed act) of theft or degradation of intellectual or real property;
- "A threat (or completed act) of a violation of any 'red chapter' (heightened) policy;^[1]
- "A threat (or completed act) of any policy violation that may cause damage to the brand and reputation of

our organization;

- “A threat (or completed act) of any employee that violates a policy that pertains to the safety and security of our staff, customers, external stakeholders, or a human being anywhere; and
- “A threat (or completed act) of a violation of our honor code or integrity standard as listed in any organization policy.”

These protocols, some of which are very broad in scope, may conceivably cover everything that an executive leader would want to know from an employee who takes advantage of an ODP system. Yes, this policy speaks to an actual system within your organization, and it should be treated as such.

Your red chapter policies alone are guaranteed to cover every high-liability policy and procedure in your organization. The policy also covers brand reputation, theft, safety, and security. Obviously, depending on the size and breadth of your organization, the list may need adjusting, but you can make the adjustments as needed.

The policy can also state what it should not be used for by introducing a “prohibitive list.” Including this clause, however, depends on several nuances of your organization, such as the company size, what it does, and historical context in terms of unionization, relationship between leadership and staff, and professional environment, etc. Although, I would usually make the argument that there shouldn’t be a need to prescribe what not to do.

This document is only available to members. Please [log in](#) or [become a member](#).

[Become a Member](#) [Login](#)