Confidentiality

"We are obligated to protect confidential and proprietary information, whether generated by USP or by third parties, unless disclosure is authorized or legally mandated."

In carrying out USP activities, employees, volunteers, and representatives often have access to confidential information. We are obligated to protect confidential and proprietary information, whether generated by USP or by third parties, unless disclosure is authorized or legally mandated.

All information about USP and our core and allied compendial activities is considered confidential unless it is made publicly available by USP or it is known to be publicly available outside of our organization.

We all are responsible for safeguarding confidential information.

We all are responsible for safeguarding confidential information by marking it "Confidential," keeping it secure (within USP or when accessible to volunteers), limiting access to the information, and disposing of it in an appropriate manner. Confidential information may be shared with employees, volunteers, and representatives only on a need-to-know basis. Failure to adequately protect confidentiality may result in significant competitive or legal harm to USP or third parties.

SOPs, with respect to the protection of confidential and proprietary information, are not intended to restrict employee rights to address compliance and ethics issues or other workplace concerns. Specific confidentiality provisions applicable to USP volunteers are located in the *Rules of Business Practice for the USP Board of Trustees* and *the Rules and Procedures of the Council of Experts*. USP employees must comply with the confidentiality provisions set forth in other USP SOPs.

USP employees must comply with the confidentiality provisions set forth in other USP SOPs.

Social Media

Social media provides an interactive platform for users to communicate to a broad audience on a variety of topics. Because there is no control over messaging once it has been sent, it is always a good idea to think first before posting anything on social media sites.

When engaging in social media activities on behalf of USP, you must always use good judgment and comply with the USP SOP on *Use of Social Media* and with the Code.

When engaging in social media activities on behalf of USP, you must always use good judgment and comply with the USP SOP on *Use of Social Media* and with the Code.

Although USP does not seek to restrict the personal use of social media, when engaging in social media on your own behalf, you are nevertheless obliged to comply with all USP confidentiality requirements concerning the sharing of USP information.

You should always use good judgment and:

- Make it clear that you are not acting on behalf of the USP, whether expressly or impliedly.
- Do not use your USP email address as your means of identification or for receiving or sending messages.
- With the exception of protected speech—such as on wage, hours, and working conditions—do not make negative comments about USP, refer to USP, or identify your connection to USP.
- Maintain the confidentiality of business and proprietary information.
- Respect the privacy of your colleagues.

Our Code in Action

What are examples of confidential information?

Confidential information may include but is not limited to:

- Financial information that is not required to be made publicly available
- Scientific, research, and medical information
- Donor and prospective donor information
- Customer and supplier information lists
- Commercial marketing strategies
- Certain personnel and consultant data
- Proprietary computer software and technology
- Correspondence between and among USP staff and members of its Board of Trustees, Council of Experts, and Expert Committees
- Contractor bid, proposal, and source selection information in government contracts
- Other information that USP or a third party deems confidential