Response Guidelines and Tips for PHS Personnel
Engaging in discussion on the PHS Pharmacists Facebook page

PHS welcomes open dialogue on Facebook. Leadership, officers, and staff are encouraged to connect with each other and engage with our "fans" to share experiences and provide accurate information as part of our effort to recruit health professionals to join the Corps.

If you see a question or comment posted on the PHS Facebook page wall or any social community please adhere to these guidelines before responding.

- **Transparency:** Disclose your relationship to the Corps.
- **Tone:** Use casual, friendly language that reflects highly on the Corps.
- **Accuracy:** Double check for accuracy. Stay within your lane and do not comment on topics that are outside your area of expertise.
- **Source:** Provide a link to more information. Link to a specific page on the PHS Web site.
- **Follow-up:** Return to your response within 24 hours and follow-up if needed.
- **Referral:** Direct comments or inquires that are personal in nature or media inquiries to appropriate personnel through official channels. Refer recruiting or application inquiries to 800–279–1605. Refer active duty Officers to call 877-463–6327.

Never solicit personally identifiable information or engage in personnel/HR conversations within social communities.

If in doubt, please consult with your Facebook Account Managers:

CDR Kendra Stewart
Email: Kendra.Stewart@fda.hhs.gov
(240) 276-8998

CDR Laura Pincock
Email: Laura.Pincock@fda.hhs.gov
(301) 796-0522

LCDR Peter Diak
Email: Peter.Diak@fda.hhs.gov
(301) 796-0572

CDR Josephine Lyght
Email: JLyght@hrsa.gov
(301) 443-3569

General Social Media Guidelines for PHS Personnel

1. Whether or not to participate in online social environments is an individual's personal decision. PHS personnel maintain their First Amendment Rights and do have the right to express them in a public forum.

2. PHS personnel should be cognizant of how they represent themselves on personal social networking sites. Staff should never post information that could reflect poorly on PHS and should always remember that even information posted to personal profiles lives in the public domain and could be seen by others.

3. Ensuring compliance with privacy laws such as The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is paramount. Any information that violates privacy laws should not be discussed. If a person is in doubt as to whether information may violate any privacy laws, they should consult with their immediate supervisor.

4. If PHS personnel notice that others in their social networks are warning their fans, followers, friends, etc., about malicious attacks, including worms, viruses, or otherwise, personnel should vet the accuracy of the warning, repost on their personal social networks and relay the information to CDR Stewart.

5. PHS personnel should relay advisories related to malicious attacks or suspicious online activity issued by law enforcement or third party social networks to an account manager immediately.

6. Personnel may refer to PHS on their personal social profiles and work history, but should remember that doing so identifies them as a part of a large network that includes their colleagues and superiors. The information they post there should be consistent with their role as PHS staff and as a representative of the Commissioned Corps. It is strongly recommended Facebook profiles be marked as private.