# Stony Brook Medicine Graduate Medical Education

| | |
|---|---|
| **Subject**: GME0034 Social Networking Policy | **Published Date:** 06/20/2023 |
| Graduate Medical Education | **Next Review Date:** 06/20/2026 |
| **Scope:** SBM Stony Brook Campus | **Original Creation Date:** 01/28/2013 |

Printed copies are for reference only. Please refer to the electronic copy for the latest version.

## Responsible Department/Division/Committee:

Graduate Medical Education Committee

## Policy:

Stony Brook Medicine Residents and Fellows utilize social network sites in a responsible and professional manner. They adhere to the guidelines set forth in this policy whether they are participating in social networks personally or professionally and whether they are using personal or SBM computing equipment.

## Definitions:

**Social Networking Site –** Internet-based applications that support and promote the exchange of user-developed content. Such content can be text messages (MMS), media messaging, Twitter, Facebook, Linked-in, TikTok, YouTube, Instagram, Snap Chat, Pinterest, Reddit, and all other social network platforms, personal and organizational websites, blogs, wikis and similar entities.

**Protected Health Information (PHI)** -
An individual's oral, written or electronic health information created or received by a Covered Entity, that is identifiable or for which there is a reasonable basis to believe that the information can be used to identify the individual, and relates to 1) the past, present, or future physical or mental health condition of an individual, or 2) the provision of health care or payment for health care to an individual. HIPAA details the below 18 identifiers that render health information identifiable:

1. Names

2. All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code in certain situations.
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
4. Telephone numbers;
5. Fax numbers;
6. Electronic mail addresses;
7. Social security numbers;
8. Medical record numbers;
9. Health plan beneficiary numbers;
10. Account numbers;
11. Certificate/license numbers;
12. Vehicle identifiers and serial numbers, including license plate numbers;
13. Device identifiers and serial numbers;
14. Web Universal Resource Locators (URLs);
15. Internet Protocol (IP) address numbers;
16. Biometric identifiers, including finger and voice prints;
17. Full face photographic images and any comparable images; and
18. Any other unique identifying number, characteristic, or code.

**Electronic Protected Health Information (e-PHI)** – Any information, defined as protected health information that is contained, maintained, transmitted, stored used, disclosed or shared in electronic format/media.

## Procedures:

The following guidelines outline appropriate standards of conduct related to all electronic information (text, image or auditory) that is created or posted externally on social media sites by personnel affiliated with GME.

### Take Responsibility and Use Good Judgement.

Be responsible for the material you post on Social Networking Sites. Be courteous, respectful, and thoughtful about how other Stony Brook employees or patients may perceive or be affected by the posting. Inaccurate, inappropriate, threatening, harassing or poorly worded postings can be harmful to others. Negative posts can damage relationships, undermine Stony Brook's reputation, discourage teamwork, and negatively impact Stony Brook's commitment to patient care, education, outreach and community service.

## Protect Others' Privacy

Content Involving Patients: Do not disclose PHI. Disclosing information about patients without a patient's written authorization, including photographs or other identifiable information, is strictly prohibited. This rule also applies to deceased patients and includes any and all social posts, including those in the secure/"friends only"/"limited audience" section(s) of your social network site/page.

Content Involving Colleagues: Employee, trainee, resident and fellow privacy is also paramount. Ask for permission before including their likeness on social media; do not disclose confidential information (location, title, IDs, etc.); and take note of your surroundings.

## Protect Proprietary Information

Do not share confidential or proprietary information. This ensures SBM's business practices and/or information security are not compromised. Similarly, do not share information in violation of any state and/or federal laws or SBM policies.

## Do Not Offer Medical Advice

Do not misrepresent your qualifications. As a trainee, provision of medical advice must be supervised by a licensed physician at all times.

## Do Not Conduct University Business Unless Authorized.

Only University employees authorized by their departments may use social networking websites to conduct University business. If authorized and in keeping with University policy, an employee may post on a social network profile: the University's name, a University email address or University telephone number for contact purposes, or post official department information, resources, calendars, and events.

*For example, a student health advocate or educator is charged with student outreach and education within their job description. Student Health Services may authorize these employees to use an on-line social network site to communicate with students and post University resources.*

If a resident or fellow wishes to create a social media page/account/profile for their residency program, they must first be granted permission by the Director of Graduate Medical Education. This is to avoid duplicate accounts and ensure bandwidth and overall success. Additionally, all resident and

fellow-run accounts must make clear in their account bio/"about" section that the accounts are resident or fellow-run. Furthermore, residents and fellows do not need to post as frequently or as formally as best practices would require, however, these accounts are not permitted to use any Stony Brook marks or branding (such as logo treatments, the shield, the Seawolf, red rays, etc.) that would produce a strong and legitimate affiliation with Stony Brook University or Stony Brook Medicine. These accounts must also have something in their handle/username (and profile photo, if applicable) that makes clear they are a residency program (e.g. residents, residency). And lastly, although going this route allows for greater flexibility in post frequency, it does not excuse residents and fellows from abiding by the other rules set forth in this policy.

If a resident or fellow wishes to have an official, Stony Brook-recognized presence on a social media platform, they must fill out the Stony Brook Medicine Social Media Account Request Form for consideration. If approved, account managers must follow best practices and go through a training with the Senior Manager, Social Media and Engagement. They are also required to review IM0076 Social Networking Sites and provide the Senior Manager with account login credentials/admin access.

**Use Caution If Expressing Personal Views.**

Individuals or groups within the Stony Brook community are not permitted to present personal opinions in ways that imply endorsement by the University. If the posted material may reasonably be construed as implying the support, endorsement, or opposition of the University with regard to any personal statements, including opinions or views on any issue or if the poster's Stony Brook affiliation is evident in the posting, the material shall be accompanied by a disclaimer that the individual is speaking for himself or herself and not as a representative of the University or any of its offices or units. An example of a disclaimer is as follows:

*The contents, including all opinions and views expressed, in my profile [or on my page] are entirely personal and do not necessarily represent the opinions or views of anyone else, including other faculty, students, or staff in my department or at Stony Brook University. Stony Brook University has not approved and is not responsible for the material contained in this profile [or on this page].*

**Be Aware of Relevant University Policies.**

Postings on social network sites are subject to the University's policies, including but not limited to, the Code of Student Conduct, Sexual

Harassment and Use of Technology policy. Students may be subject to disciplinary actions for violations of University policy, up to and including dismissal or termination.

Failure to abide by SBM policies are subject to disciplinary actions, in accordance with policy GME0009 Substandard Resident Performance.

These guidelines include, but are not limited to: Use and Disclosure of Protected Health Information (PHI) or Confidential SBM Material(s); Appropriate Computer Use; Use of SBU Trademarks and Proprietary Information; Electronic Communications; Confidentiality of the Medical Record; Camera and Video Recorder Use; Use of Portable Electronic Devices.

**Forms: (Ctrl-Click form name to view)**

Stony Brook Medicine Social Media Account Request Form

**Policy Cross Reference: (Ctrl-Click policy name to view)**

IM0076 Social Networking Sites

IM0060 Workforce Security Related to Electronic Protected Health Information (e-PHI) User Access Authorization

LD0058 Review of Suspected Health Insurance Portability and Accountability Act (HIPAA) Violations

RI0036 Notice of Privacy Practices

RI0050 Photography/Videography, Voice Recordings of Patients, Visitors and Workforce Members

**Relevant Standards/Codes/Rules/Regulations/Statutes:**

Health Insurance Portability Act 1996 (HIPAA) Security Rule