

## **New Temporary Policy and Process for Visitors/Vendors (for non-patient-related visitors)**

As you know, during these times of COVID-19, we need to be careful about who we let into the building, and we need to be sure not to let people access clinical floors unnecessarily. That said, we also know that we will need to host special guests from time to time. Therefore, please review the following policy for visitors who are here for business other than as a patient or patient companion. Until further notice, here are the steps you need to take if you would like to host someone at One Kneeland:

### **All visitors and entrants need to satisfactorily complete a health screening before being admitted to the building.**

All visitors and entrants must show and submit documentation of COVID vaccination and booster before being admitted to the building. Tufts University is requiring all vendors and affiliates to attest that they have received a Booster Shot based on the eligibility per CDC guidance. [COVID-19-vendor-affiliate-policy-Booster-FINAL.pdf](#) | [Powered by Box](#)

At least one week before the visit, please provide Jill LeClare at [Jill.Leclare@tufts.edu](mailto:Jill.Leclare@tufts.edu) with the following information:

Vendor/visitor name:

Vendor/visitor email address:

Vendor/visitor phone number:

Company/Organization:

Date(s) of visit:

Expected Arrival Time:

Department Visiting:

Areas of the School to be Accessed:

Purpose of Visit (briefly):

Tufts Dental Contact Name:

Tufts Dental Contact Best Phone# to Reach on the Day of the Visit:

Proof of COVID vaccination submitted to Jill LeClare

Jill will then generate the Health Survey that must be completed by the visitor no more than two hours prior to his/her entry to the School. The name will be added to the expected visitor list. Your guest will undergo a Health Screening upon arrival. You, as the host, must meet your guest in the lobby and escort them to the appropriate venue.

Depending on the nature of the visit, your guest may also be required to complete a "TUSDM Confidentiality and Information Security Agreement" in advance of the visit.

If there is a possibility your guest will visit a clinic or have access to protected health information (PHI), your guest must read, sign, and return the following:

**TUSDM Confidentiality and Information Security Agreement**

All Tufts University School of Dental Medicine (“TUSDM”) Workforce Members, including faculty, staff, students, volunteers, and interns (regardless of whether they are TUSDM trainees or rotating through TUSDM from another institution), as well as TUSDM-sponsored Visitors observing within the clinic areas, and other individuals who perform work for TUSDM, are personally responsible for ensuring the privacy and security of all confidential patient, employee, and business information.

**I understand and acknowledge the following:**

**Policies and Regulations:**

1. I will comply with all Tufts University and TUSDM policies governing protected information.
  - Privacy: <https://dentalpolicies.tufts.edu>
  - Information Security: <https://it.tufts.edu/ispol>
2. I will timely complete all privacy and security training required of my position within the TUSDM workforce.
3. I will report all concerns about inappropriate access, use, or disclosure of protected information, and suspected policy violations, to the TUSDM confidential hotline 866-384-4277, or via email at [Dental-Compliance@tufts.edu](mailto:Dental-Compliance@tufts.edu)
4. I will report all suspected information security incidents and information security policy violations to the TUSDM HIPAA Information Security or Privacy Officers or the Tufts Information Security team at 617-627-6070 or [Information\\_Security@tufts.edu](mailto:Information_Security@tufts.edu).

Patient Health Information (“PHI”) includes: Information that relates to the past, present, or future health of an individual, including the provision of healthcare to an individual and payment for the provision of healthcare, which identifies, or reasonably could be used to identify, the individual, and which is transmitted or maintained in any other form or medium (electronic, paper, verbal, etc.) Examples include, but are not limited to:

- any information about the patient’s physical or psychological condition/health status,
- verbal information overheard or provided by or about a patient, and
- visual observations of patients receiving medical care or accessing services at TUSDM.

**Confidential Personal Information (“PI”) includes, but is not limited to the following:**

A person’s first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to the individual:

- Social Security number, Driver’s license number or State-issued identification card number;
- financial account number or credit or debit card number with or without any required security code, access code, personal identification number, or password that would permit access to an individual’s financial account; and
- other such information obtained from Tufts University or TUSDM records which, if disclosed, would constitute an unwarranted invasion of privacy.

**Confidentiality of Information:**

5. I will access, use, and disclose PI and PHI, including paper or electronic records, only to perform my assigned duties or educational activities and in a manner consistent with the policies and procedures of Tufts University and TUSDM. I will limit my access, use, and disclosure of PI and PHI to the minimum amount necessary to perform my authorized duties or educational obligations. I understand that my access will be monitored to assure appropriate access, use, or disclosure.
6. I will maintain the confidentiality of all PI and PHI to which I have access.
7. I will not discuss confidential information with any unauthorized persons. When required as part of my work or education-related duties or activities, I will make every effort to discuss confidential information in non-public areas.
8. I will take all reasonable steps to keep patient information out of view of patients, visitors, and individuals who are not involved in the patient's care.
9. I will use Tufts University and TUSDM resources, including computers, email, photography, video, audio, or other recording equipment only for job-related duties or for duties/actions expressly permitted by applicable Tufts University or TUSDM policy: <https://it.tufts.edu/ispol>
10. I will not take PI or PHI off the TUSDM campus, for any reason, unless expressly permitted by the TUSDM Privacy Officer. Should I be given permission to take PI or PHI offsite, I will keep the PI or PHI fully secured and in my physical possession during transit, never leaving it unattended or in any mode of transport (even if the mode of transport is locked).

#### Computer, Systems, and Electronic Health Record Access Privileges:

11. I will only access the records of patients for job- or education-related duties or activities.
12. I will not electronically access the records of my family members, including minor children, except for assigned job- or education-related duties.
13. I will protect access to patient and other job- and education-related accounts, privileges, and associated passwords:
  - I will use a strong password on my computer, laptop, and smartphone.
  - I will commit my password to memory or store it in a secure place.
  - I will not share my password.
  - I will not log on for others or allow others to log on for me.
  - I will not use my password to provide access or look up information for others without proper authority.
14. I am accountable for all accesses made under my login and password, and any activities associated with the use of my access privileges.
15. I will only use my own credentials in accessing patient accounts and/or systems as provided to me for my job- or education-related duties and activities.

#### Computer Security:

16. I will store all PI or PHI on secured systems, encrypted mobile devices, or other secure media.
17. I will not change my TUSDM computer configuration unless specifically approved to do so.
18. I will not disable or alter the anti-virus and/or firewall software on my TUSDM computer.
19. I will log out or lock computer sessions prior to leaving a computer.
20. I will not download, install, or run unlicensed or unauthorized software on University-issued media.

21. I will use administrative permissions only when I am approved to do so and when required by job function.
22. If I use a personally owned computing device for TUSDM functions, I will not connect it to a TUSDM network unless it meets the same security requirements as a TUSDM-issued or owned device.

**TUSDM Confidentiality  
and Information Security Agreement  
Signature Page**

The preceding materials are for the TUSDM student or sponsored Visitor to keep.

This signature page for the TUSDM HIPAA Confidentiality and Information Security Agreements to be removed from the document and turned in to the manager of the TUSDM sponsoring/hosting clinic or department.

My obligation to safeguard patient confidentiality and protected information continues even after I am no longer a TUSDM Workforce Member or my work performed on behalf of TUSDM has concluded.

**I acknowledge that I have read and understand the foregoing information and that my signature below signifies my agreement to comply with the conditions imposed above. I further understand that failure to comply with this agreement may result in disciplinary action up to and including termination of my status as a TUSDM Workforce Member or TUSDM-sponsored Visitor. Additionally, there may be criminal or civil penalties for inappropriate uses or disclosures of certain protected information.**

Signature: \_\_\_\_\_ Date:

Print Name:

Company/Department:

Hosting Clinic/Department:

Email Copy of Signature Page to:

TUSDM Security and Privacy Officer

Jill LeClare

[jill.leclare@tufts.edu](mailto:jill.leclare@tufts.edu)