University of California
San Francisco

Privacy Guidance for MD Link Members

Protecting the privacy and confidentiality of patients' health information is a fundamental ethical concept and requirement in healthcare. When you joined UCSF's MD Link program you agreed (whether in the Terms and Conditions, the Participation Agreement, and/or the Confidentiality Statement you signed) to protect health information as required by federal and state law. To ensure you are adhering to all applicable rules and regulations please review and follow this guidance carefully.

Accessing Records in a Proper Manner

Limit your access to what is necessary for business reasons. State and federal law requires that you limit your access to patients' medical records to those instances when you have a business reason to view, access, or modify records a patient's information. This means that you must have a treatment relationship with the patient and have a need to access the information at the time the access occurs. Examples of inappropriate use of MD Link are:

- Searching for, and/or accessing records of, your friends, family, or co-workers' medical records
- Searching for, and/or accessing records, for research purposes
- Searching for contact information of individuals you know or want to contact
- Accessing more of a patient's record than is necessary for non-treatment purposes

Using and Disclosing Accessed Information

Maintain confidentiality of accessed information at all times. You have a duty to keep confidential any and all information you view or acquire through MD Link. This applies to information about your patients as well as information you view incidental to your work. To prevent unauthorized disclosures, do not use information you view or acquire through MD Link in the following manners:

- Do not post or discuss patients' identities or health information on social media or other public forum
- Do not share information with entities or individuals unless it is for treatment, payment, or operations purposes as defined by federal and state law

Preventing Data Breaches

Ensure you have proper technical, physical, and administrative safeguards in place. Protecting data is an important part of privacy regulations. All entities who store health information are required by federal and state law to have appropriate data security in place.

- Encrypt all electronic devices that come into contact with health information
- Do not leave the MD Link portal open when not using it — this will prevent unauthorized use
- Train your workforce on privacy and confidentiality rules and regulations
- Refer external entity requests for UCSF records to UCSF Medical Records Department at (415) 353-2221 — do not release UCSF's records
- Notify UCSF Privacy Office at (415) 353-2750 if you discover a potential breach of UCSF information

Contact UCSF with Questions

- For privacy questions contact the UCSF Privacy Office at privacy@ucsf.edu or at 415-353-2750
- For questions regarding MD Link contact Brian Cosgrove at Brian.Cosgrove@ucsf.edu

Updated February 2015