

Name of Policy: [Photographing, videotaping, filming, video recording](#)

Policy Number: 33640-14

Approving Officer: President

Effective date:
September 1, 2023

Responsible Agent Privacy Officer and Director of
Health Information Management

Scope Hybrid and affiliated covered entity of University
of Toledo

- (c) Use of equipment should not disrupt or create a safety concern or violate the privacy of other employees, patients, or visitors

(F) Electronic media

Electronic transmission is permitted if sent from a secured connection. The university of Toledo information technology department should be consulted prior to electronic transmission to ensure that secure connections are incorporated and assured. Transmission of photographic images may only be shared with those who are involved with the patient's care, such as but not limited to, attending physician/faculty or other clinical personnel.

- (1) In order to protect the patient's confidentiality, photographs sent via the internet/telemedicine must be encrypted, along with any attached medical information, prior to sending.
- (2) Stream video may only be transmitted from a secure server to another secure site/web page where the viewing requires password login to view the images.
- (3) No photographs including stream videos shall be shared by electronic media such as but not limited to facebook, twitter or other social networks.

(G) Destruction, de-identified, disclosure, documentation storage and retention of photographs

(1) Destruction

- (a) Photographs taken for purposes of documenting in the medical record should be downloaded and maintained by the Health Information Management Department. Once downloaded the image must be destroyed within a reasonable time frame and in a manner that the photograph may not be reconstructed at a later date. This includes all equipment that is capable of taking/producing photographs or video (see University Policy

#336490-16, Medical Record Retention and Destruction (Disposal of Protected Health Information).

- (b) All other photographs taken for teaching, staff development and medical/healthcare education should be de-identified or a consent should be maintained on file.
- (c) De-identified is defined in Policy #336400-90-05, de-identifiable and re-identifiable health information. The policy requires that all patient data that would identify the patient be removed from the photograph or not included in the photograph, such as patient's face, medical record number, room number, account number or any other identifying attribute that could identify the patient.

(2) Disclosure

Unless otherwise required by federal or state law, photographs will not be released to outside requestors without a specific release from the patient or his/her legal reprt

(H) Kobacke adolescent and child psychiatry