COMPLIANCE 9.1 FACILITY SURVEILLANCE VIDEO CAMERA RECORDING

Scope: All subsidiaries of Universal Health Services, Inc., including facilities, Independence Physician Management (IPM), Prominence Health Plan and UHS of Delaware Inc. and their personnel.

Purpose: To provide direction for retention and destruction of video surveillance recordings in the facility.

Procedure:

A. Storage time for video surveillance footage is subject to overwrite capabilities of the individual system but generally should not exceed 30 days.
B. DVRs should be maintained in a secure location with access limited only to the Director of Plant Operations, Security, Risk Manager and the CEO.
    a. The CEO can determine additional designees as appropriate.
C. The determination of whether to copy/burn camera surveillance recorded images is limited to the Facility CEO, Facility Risk Manager, UHS Compliance, UHS Claims, and UHS Office of General Counsel. These individuals/departments can enlist other departments, i.e. Security, Information Services to assist in securing the records.
D. Review of/Access to camera surveillance live feed or recorded images from a remote/off-campus location or device is strictly prohibited.
E. Retrospective camera surveillance video viewing should be restricted to the CEO, the Facility Risk Manager, the Chief Nursing Officer/DON, the Director of Security (Acute Division) as appropriate, and to Corporate Claims, as necessary in connection with active or threatened litigation. Additional personnel, where appropriate should access recorded video footage in the physical presence of the CEO and/or Facility Risk Manager. Other senior management personnel (COO, CFO, etc.) are appropriate substitutes for the CEO and Risk Manager if they are unavailable.
F. Video footage from surveillance cameras at a facility should be maintained and uploaded to the secure portal under the following circumstances:

    i. If such footage is related to an Adverse Event Report (AER) and/or for liability claims, if available;
    ii. Where the facility is on notice of litigation, threat of litigation, other legal action, or an investigation by any administrative, civil or criminal authority, through the receipt of notification or other information identifying the possibility of legal action or upon service of a summons and complaint and video footage is available and can be reasonably identified. See **Legal Holds and Electronic Data Preservation, Legal 6.0. and Legal Holds and Electronic Data Preservation, Insurance 1.18.**
    iii. For significant patient injuries as a result of a restrictive intervention, if available; and

iv. For any additional incidents in which the facility may have exposure for potential legal claims such as employee claims or injuries, as may be determined by facility risk management and Regional Loss Control.
v. For any videos released pursuant to a valid court order / subpoena, the video footage should remain on the secure site

Absent these circumstances, video from surveillance cameras is subject to routine overwriting in accordance with the applicable software.

G. If available, video footage meeting the criteria described in section F, shall be uploaded to the secure portal with the assistance of Corporate IT for access by the Claims/ Insurance Department as directed by that department.

   Below is the labeling protocol for videos:
   a. Videos for a specific AER: AER #; Name of Facility
   b. Near Misses/Incidents: YYYYMMDD Incident; Name of Facility
   a. Other potential claims or employment related matters: YYYYMMDD Other; Name of Facility

H. No preserved video footage of an alleged incident/event will be maintained at the facility.
I. If video footage is used for training of staff, the video footage in question should be reviewed in real time or within 30 days.
J. In the course of an investigation, police and/or state licensing departments may request the video footage. If the video footage still exists in the facility's system, it is acceptable for the Risk Manager to show the video to the investigating agency or officer, with the proper authority. If the video exists in the secure portal, contact regional Risk, Claims, Legal, or the Compliance Office, as appropriate, for advice.
K. In order to ensure compliance with all privacy laws and regulations and to avoid potential improper retention, duplication or unintended dissemination of retained video footage, any copies of such footage retained in accordance with this policy should be destroyed in such a manner so the copy is not accessible or viewable. No copies of the video footage should be maintained or distributed to anyone either inside or outside of the facility beyond the guidance and instructions in this policy. Additional guidance on the use photographs and/or recordings of patients can be found in **UHS Privacy 13.0 *Photographs, Videotapes, and Other Recordings*.**
L. Please note that if you are using a USB when making copies of video footage, you must use a UHS corporate approved encrypted USB device, consistent with applicable UHS Security policy. Passwords must not be sent with the USB device. Passwords will need to be sent via an outside channel such as an email or phone call.
M. Inappropriate destruction, retention or dissemination of video footage in violation of this policy may lead to correction action up to and including immediate termination.
N. All questions pertaining to this policy should be addressed to the UHS Compliance Office.

Related UHS Policies:

UHS Privacy 13.0 *Photographs, Videotapes, and Other Recordings*

UHS Privacy 16.0 *Disclosures for Law Enforcement Purposes*

UHS Security 2.03.05 *Data Encryption and Decryption*

UHS Legal 6.0 *Legal Holds and Electronic Data Preservation*

Insurance, 1.18, *Legal Holds and Electronic Data Preservation*

Revision Dates:

12-30-2011; 10-01-2015; 10-4-2017; 10-26-18;

5-24-2021; 11-29-2021

Implementation Date: 12-30-2011

Reviewed and Approved by:

UHS Compliance Committee