

UC Davis Health has recently experienced a notable increase in fax phishing attempts (“fax-ishing”). This document is intended to alert the UC Davis Health workforce about this situation and provide information for if it is encountered.

### WHAT IS FAX-ISHING?

Traditional phishing is electronic in nature through emails and text messages; however, phishing may also occur through faxes that are sent directly to our organization. This is referred to as fax-ishing. The attackers pose as legitimate companies, send faxes to different UC Davis Health locations, and seek to trick our workforce into sharing our patients’ information or confirming that someone is a UC Davis Health patient.

Using a fishing analogy, scammers use faxes as lures, strategically placing bait to “fish” for responses from the UC Davis Health workforce that will include the disclosure of patient information. In this analogy, a fax-ishing attack is comprised of four essential elements: the phisher, the phish, the bait, and the hook.

#### THE PHISHERMAN

This element refers to the attackers, looking to carry out a phishing attack. The attackers strategically target UC Davis Health with the explicit goal of acquiring patient information. It is crucial for our workforce to confirm the validity of external faxes that request patient information.

#### THE PHISH

The “phish” element in these attacks refers to our workforce members who are tricked by the attackers’ bait. Since UC Davis Health creates and maintains protected health information, the

enterprise will likely continue to experience ongoing fax-ishing attempts.

#### THE BAIT

This element is the content within the fax, skillfully crafted by attackers to entice or lure our workforce into responding. These attackers consistently use a variety of diverse tactics such as posing as legitimate companies to deceive our workforce. Notably, fax-ishing may include accurate patient identifiers and may be directed to the correct provider, enhancing their apparent legitimacy.

Fax-ishing attackers use a variety of tactics to enhance the appearance of authenticity.


Urgency is a common ploy, with the attackers urging the need for an immediate response. We have received confirmation from clinics that some attackers will often follow-up with phone calls, intensifying the sense of urgency of the request.

#### THE HOOK

The ultimate goal of fax-ishing is to gain access to patient information. The information can be used for insurance fraud or other malicious purposes.

**Questions?** Please contact the Privacy Program team with related inquiries or concerns.

 [hs-privacyprogram@ucdavis.edu](mailto:hs-privacyprogram@ucdavis.edu)

 (916)734-8808

## HOW TO AVOID FALLING VICTIM TO A FAX-ISHING ATTEMPT


### Verify the validity of the requestor.


- If the requestor is a known company, do the phone and fax numbers match the numbers we have in our system?
- Contact the company through a trusted and known contact method if the fax is questionable.
- Fax-ishing telephone numbers often go directly to a generic voicemail.


### Is the request inconsistent with care provided to the patient by UC Davis Health? If yes:


- Please reach out to the patient to validate their awareness of the request.
  - If the patient is aware of the company/request, staff should document this in the patient's EMR, and the provider should review if the request is medically necessary.
  - If the patient **is not** aware of the company/request, staff should report it as potentially fraudulent by submitting an incident in RL Datix or emailing Compliance and Privacy Services to document the receipt, the reporting, and to maintain a scanned copy of the request.

#### Three ways to report privacy incidents:

 [hs-privacyprogram@ucdavis.edu](mailto:hs-privacyprogram@ucdavis.edu)

 (916) 734-8808

 Submit an Incident Report through RL Datix by typing "incident" in your browser address bar or login through Citrix.

 Select "Confidentiality/Healthcare Information" category when completing the report.

### A LOOK AT TWO RECURRING FAX-PHISHING COMMUNICATIONS SENT TO UC DAVIS HEALTH

#### Durable Medical Equipment Orders or Prior Authorization for Durable Medical Equipment

Several UC Davis Health clinics have reported the continued receipt of fraudulent fax orders for durable medical equipment (DME). These fraudulent orders appear to come from legitimate companies, they may be directed to the patient's correct provider, and may contain accurate patient identifiers. The DME document claims that the provider or the patient requested the equipment and requests the patient's diagnoses along with the provider's signature. The targeted clinics have reported that the attackers will often call the clinics to check the status of the claim.

#### HIPAA Compliant Physician Form or Active Patient Confirmation Form

Some of our clinics have also reported receipt of multiple fax-ishing attempts through forms titled *HIPAA Compliant Physician Confirmation Form* or *HIPAA Compliant Form to Confirm an Active Patient*. Similar to the DME phishing forms, some of these faxes appear to have come from legitimate companies and contain accurate patient identifiers. These communications request the provider's signature to attest the patient receives services at UC Davis Health; additionally, they seek to obtain visit notes/medical records.