

Drug Topics® Survey Identifies Patient Portal Trends in Pharmacy

A recent Drug Topics® survey gauged the ways that pharmacies are protecting patient identity and ensuring secure access

A recent survey conducted by *Drug Topics*® assessed how pharmacies are diversifying their online services, enhancing patient experience, integrating management systems, and keeping patient information safe from fraudulent behavior.

The survey received nearly 500 responses from pharmacists spanning all segments of the industry, including independent, specialty, health system and retail; however, most respondents represented independent pharmacy, at 32.4%. Nearly 29% of respondents were from a national retail pharmacy chain and 17.6% came from health system pharmacies.

Responses demonstrated that pharmacies are providing diverse online services to their customers, primarily prescription refills (83.4%) and immunization scheduling (56.5%). Other services included home delivery (47.0%), medication synchronization services (45.6%), and virtual medication therapy management (MTM) counseling (24.9%).

Some pharmacies are now offering their customers the option to fill their prescriptions through a patient portal. A patient portal provides myriad benefits, like saving customer and staff time and streamlining communication to boost patient education. According to the survey results, there is room for improvement for patient portal use in pharmacy. Approximately 35% reported that less than 10% of their patients use a portal for filling prescriptions, while another 31% reported that between 10% and 25% take advantage of a patient portal. Twenty-three percent reported that between 25% and 50% of patients access the portal for filling scripts, and only 2.9% said that more than 75% of their patients fill prescriptions through an online portal.

The survey additionally showed that pharmacies are using diverse identifiers to verify patient identity during a patient portal transaction, but most utilize patient name (82.6%)

and date of birth (82%). Other common methods include prescription number (55%) and phone number (48%). Some of the less used identifiers were email (31%), an internally created patient ID (14.6%), payment information (10.5%), and social security number (4.7%).

Respondents reported the kinds of data that is stored within their patient portal. Of the 486 pharmacists who store patient information, most said they store at least the patient's name (439), date of birth (427), address (391), phone number (373), prescription number (366), and/or email (297).

Roughly half (56%) of respondents have a web portal that is separate from front-end, retail access. Of those individuals, 33% reported that their pharmacy management software provides the security access and integration with the pharmacy dispensing system; 20% reported that it requires web portal vendor interface for refills, prescription delivery, and other services; and 10% reported that they provide a security access solution with the option of using their own vendor(s).

About one-quarter of survey respondents said that they are planning to add web portal security access enhancements within the next year, many of whom are device authentication (46.6%), multi-factor authentication (44%) and username/password (44%). While about one-third of respondents said that their web portal security provider confirms that both the device and IP address are not associated with fraudulent activity, a surprising 56% did not know whether their provider requires dual confirmation.

The good news is that 85% of respondents have not experienced an increase in web portal attacks in the last two years. On the other hand, nearly 84% expressed at least slight concern about their patient portals facing attacks or fraudulent activity.

FIGURE 1. As for methods of protecting patient data, respondents pointed to various security measures, including:

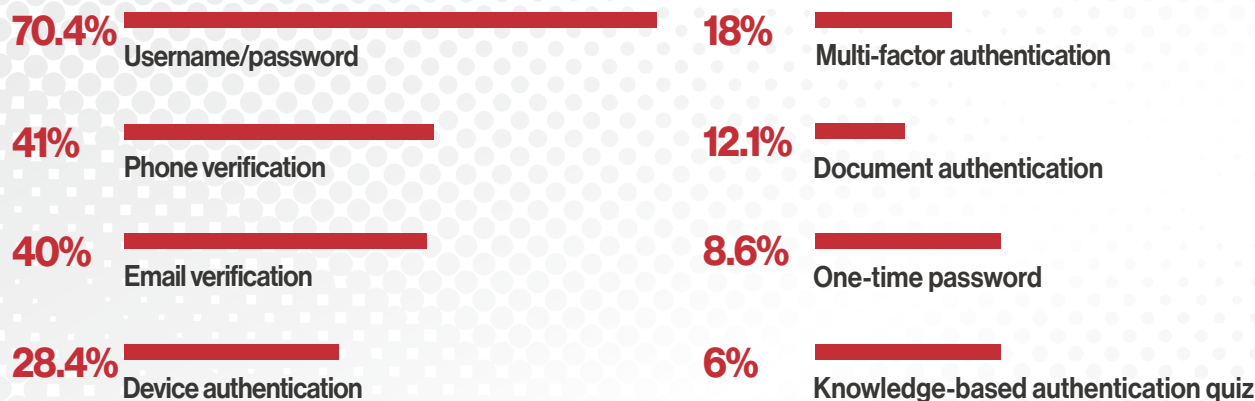


FIGURE 2. Moving forward, how concerned are you about attacks / fraudulent activity associated with your web portal?

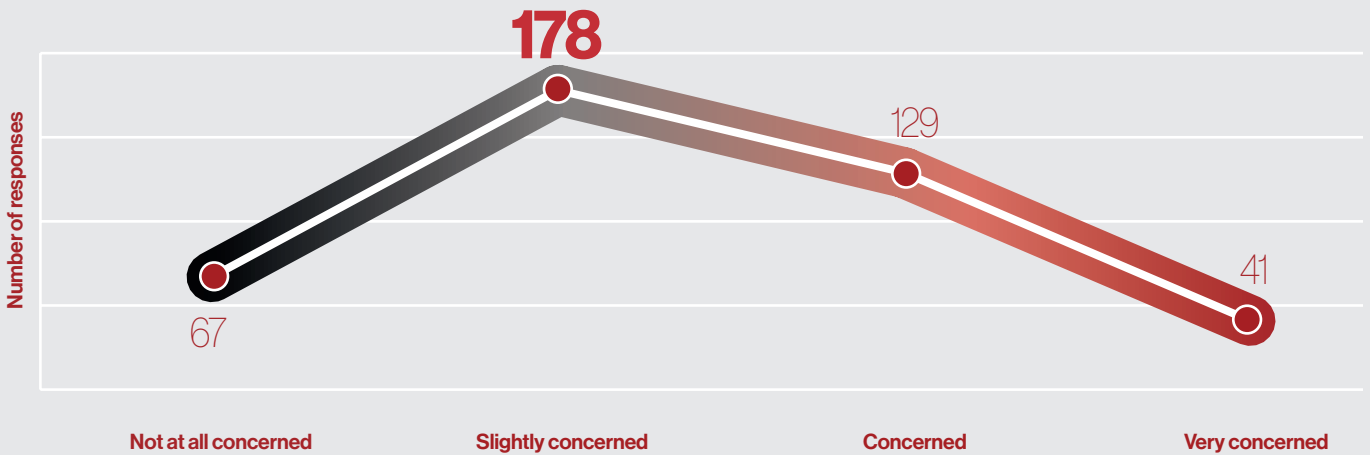


FIGURE 3. Does the pharmacy have a separate web portal from the front-end (retail) of your business, or would one sign-on enable access to both pharmacy and front-end business?

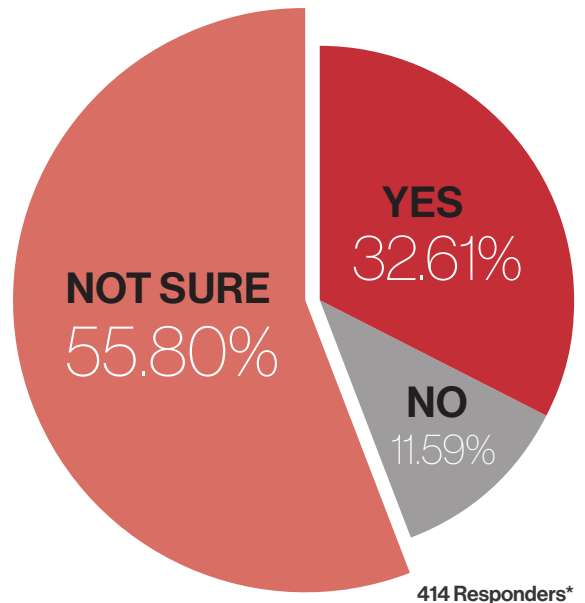
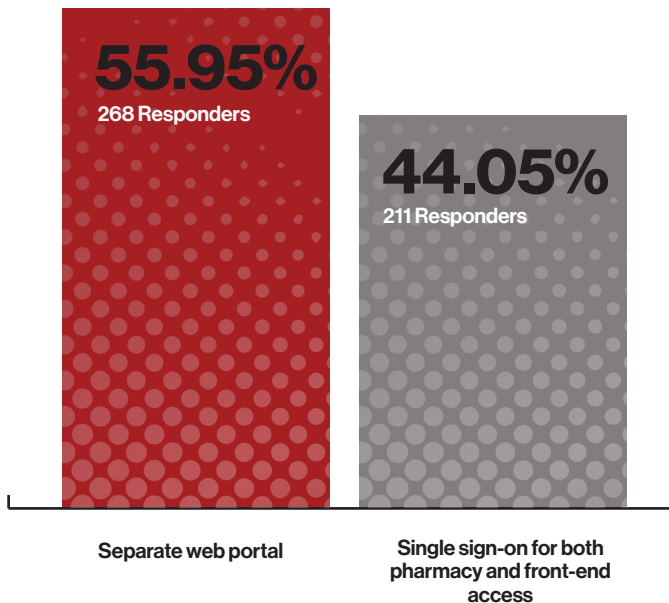


FIGURE 4. Aside from confirming user identity, does your web portal security provider confirm that both the device and location (IP address) are not associated with fraudulent/bad actors?