doi:10.36849/JDD.9297e

Enhancing Patient Privacy in Dermatology: Best Practices for Image Organization and Security

Ryan Koch MD,[a] Kritin K. Verma MBA,[b] Sino Mehrmal DO,[c,d] Stanislav N. Tolkachjov MD[c,d,e]

[a]Department of Internal Medicine, Baylor Scott & White Medical Center, Temple, TX
[b]Texas Tech University Health Sciences Center School of Medicine, Lubbock, TX
[c]Epiphany Dermatology, Dallas, TX
[d]Division of Dermatology, Baylor University Medical Center, Dallas, TX
[e]Department of Dermatology, University of Texas at Southwestern, Dallas, TX

To the Editor:

The increasing use of digital images in dermatology for diagnostic and treatment purposes presents serious privacy and security concerns. Dermatologists routinely collect and retain photos of skin disorders, both cutaneous and histopathological, to make accurate diagnoses and plan treatments. However, the possibility of these photos being compromised by cyberattacks necessitates strict security measures.[1]

Common image formats used in dermatology include Joint Photographic Experts Group (JPEG) and Tag Image File Format (TIFF). While each format has benefits, neither format naturally has security mechanisms to prevent unwanted access.[1] Regardless of format, all photographs should be encrypted and password-protected.[1]

Images should be kept on secure servers with strong access controls.[2] Dermatologists should avoid storing sensitive photos on personal devices because of the heightened danger of data breaches.[2] However, if a personal device is encrypted and includes adequate access control measures (eg, strong passwords, remote-wipe capability), it may be compliant with the Health Insurance Portability and Accountability Act (HIPAA). If photographs must be recorded on a smartphone, they should be uploaded to a secure server and the original deleted.[2] Additionally, employing secure cloud storage solutions with end-to-end encryption (E2EE) can help protect patient privacy as the sender securely codes data, which can only be decoded by the intended receiver.[2] Platforms like Microsoft Teams with Microsoft 365 Business or Dropbox Business offer HIPAA-compliant storage with E2EE.

In addition, photos automatically contain metadata stored with the image. Metadata refers to additional data embedded within an image file, including details such as the date and time the photo was taken, camera settings, geolocation data, and device information.[3] Geolocation data may be deactivated before pictures are taken by turning off the camera application's location services, or may be removed manually after a picture is taken.

Efficient naming conventions for images can aid in organization and retrieval while maintaining patient confidentiality.[4] A best practice is to avoid any patient-identifiable information in image names. Instead, practices can use anonymized codes that reference non-identifiable details, such as "IMG" followed by a unique number and brief descriptor (eg, "IMG1023_chest_BCC"). This method ensures that images are easily searchable while maintaining anonymity.[1,4]

For devices that use secure digital (SD) cards to store images, it is essential to implement best practices to prevent data loss or theft.[5] The SD cards should be encrypted, and access should be restricted to authorized personnel.[5] Furthermore, devices capturing images should have up-to-date security software.[2,5]

The use of digital imaging in dermatology provides tremendous benefits for patient care and education, but also raises serious privacy and security concerns.[1,2,5] Dermatologists can protect patient privacy while maximizing the benefits of digital imaging by implementing security measures such as encryption, secure HIPAA-compliant storage, and metadata management.[1,2,5] As technology advances, continual monitoring and adaptation of security policies will be required to protect sensitive patient information in dermatology.

DISCLOSURES

Dr Tolkachjov is a speaker and investigator for CASTLE Biosciences, Bioventus, Kerecis, and Boehringer Ingelheim. The other authors have no conflicts of interest to declare.

REFERENCES

1. Chen Y, Esmaeilzadeh P. Generative AI in medical practice: in-depth exploration of privacy and security challenges. *J Med Internet Res.* 2024;26:e53008.
2. Khalid N, Qayyum A, Bilal M, et al. Privacy-preserving artificial intelligence in healthcare: techniques and applications. *Comput Biol Med.* 2023;158:106848.
3. Nettrour JF, Burch MB, Bal BS. Patients, pictures, and privacy: managing clinical photographs in the smartphone era. *Arthroplast Today.* 2018;5(1):57-60.
4. Generative AI in Health Care: How can we protect health information? Gastroenterology Advisor. Available at: https://www.gastroenterologyadvisor.com/features/generative-ai-in-health-care/. Accessed April 17, 2024.
5. Maleki Varnosfaderani S, Forouzanfar M. The role of AI in hospitals and clinics: transforming healthcare in the 21st century. *Bioengineering (Basel).* 2024;11(4):337.

AUTHOR CORRESPONDENCE

Sino Mehrmal DO
E-mail:..... smehrmal@gmail.com