Report on Patient Privacy Volume 19, Number 11. November 07, 2019 Checklist for Biometric Authentication

By Jane Anderson

Biometric authentication enables an organization to use two or more active or passive biometrics to provide what experts believe is highly accurate and fast authentication, with a low error rate.

The types of biometrics that organizations can implement include:

- **Voice biometrics.** This uses voice patterns—pronunciation, emphasis, speed of speech, accent—along with physical characteristics to confirm identity.
- **Facial recognition.** The best-known application of this technology is Apple's iPhone unlock feature that uses your face to unlock your phone, but "selfie matching" also can be used by organizations for authentication purposes.
- **Passive/behavioral.** This type of biometric uses machine learning artificial intelligence to match patterns of behavior, which are unique from individual to individual.
- **Device identification.** In this case, an organization can authenticate a person through the device they carry. Software and geolocation features may play a role.