## Is Your Health Plan Secure?

*Identity authentication* is a process that corroborates a person's identity prior to granting the person access to a system or digital platform. Authentication can take numerous forms, such as a password, PIN, security token, or biometric data. Access to systems that house or transmit sensitive information, including electronic protected health information ("ePHI"), typically require *multi-factor authentication* ("MFA"), such as a password and sending a verification code to the user's phone.

There are also phishing resistant forms of MFA that decrease the risk of disclosure of sensitive information to illegitimate sources. For example, phishing resistant MFA may include a password *and* a form of authentication that only the user would have, such as a software based token authenticator. Passwords and PINs are less secure when used alone, because they are a form of authentication that a person "knows" but is not an identifier specific to the person (e.g., fingerprint) or a key only in the person's possession (e.g., access token).

The U.S. Department of Health and Human Services' ("HHS") Office for Civil Rights ("OCR") recently published a newsletter revealing that 86% of cyberattacks on organizations' web or email servers stemmed from compromised passwords or credentials. Under the HIPAA Security Rule, health plans and business associates must implement authentication procedures to validate that "a person or entity seeking access to electronic protected health information is the one claimed."

The HIPAA Security Rule sets forth obligations beyond authentication procedures, including administrative (e.g., security training), physical (e.g., off site computer backups), and technical (e.g., encryption, authentication) security measures that safeguard ePHI. Importantly, compliance with HIPAA's authentication requirements may manifest differently depending on the context and particular entity's risk factors because certain systems create more vulnerabilities. For example, accessing an organization's information systems remotely is riskier than accessing the systems within the organization's network, which means additional authentication may be warranted when users access a network remotely.

Failing to comply with HIPAA can result in serious financial liability; since 2003, OCR has obtained $135,538,772 in civil penalties from 135 cases for violations of HIPAA rules. For example, in May 2023, OCR reached a settlement with MedEvolve, Inc., a business associate, for $350,000 in connection with a data breach that compromised 230,572 individuals' ePHI. In July 2023, the L.A. Care Health Plan, an agency created by the County of Los Angeles

that provides health coverage to low income residents, settled with OCR for $1.3 million for potential HIPAA violations. The HIPAA issues involved L.A. Care Health Plan members having access to other members' ePHI (name, address, member ID number) on their payment portals and receiving ID cards that belonged to other members.

HHS actively investigates and enforces the HIPAA Privacy, Security, and Breach Rules. Health plans should ensure they have up to date HIPAA policies and procedures, are conducting required HIPAA training, and documenting their HIPAA compliance practices. They should also ensure they have current business associate agreements in place. Health plans should also ensure they are conducting periodic risk assessments and implementing security policies, procedures, and actions to address vulnerabilities.

If you need assistance with HIPAA Security Rule compliance, please contact a member of our Employee Benefits and Executive Compensation Practice Group.

## Contacts

**John E. Schembari**
*Omaha*
402.231.8886
john.schembari@kutakrock.com

**Michelle M. Ueding**
*Omaha*
402.661.8613
michelle.ueding@kutakrock.com

**William C. McCartney**
*Omaha*
949.852.5052
william.mccartney@kutakrock.com

**P. Brian Bartels**
*Omaha*
402.231.8897
brian.bartels@kutakrock.com

**Ruth Marcott**
*Minneapolis*
612.334.5044
ruth.marcott@kutakrock.com

**Sevawn Foster Holt**
*Little Rock*
501.975.3120
sevawn.holt@kutakrock.com

**John J. Westerhaus**
*Omaha*
402.231.8830
john.westerhaus@kutakrock.com

**Robert J. Hannah**
*Omaha*
402.661.8667
robert.hannah@kutakrock.com

**Emma L. Franklin**
*Omaha*
402.231.8842
emma.franklin@kutakrock.com

**Aaron D. Schuster**
*Kansas City*
816.960.0090
aaron.schuster@kutakrock.com

**Jacob S. Gray**
*Minneapolis*
612.334.5053
jacob.gray@kutakrock.com