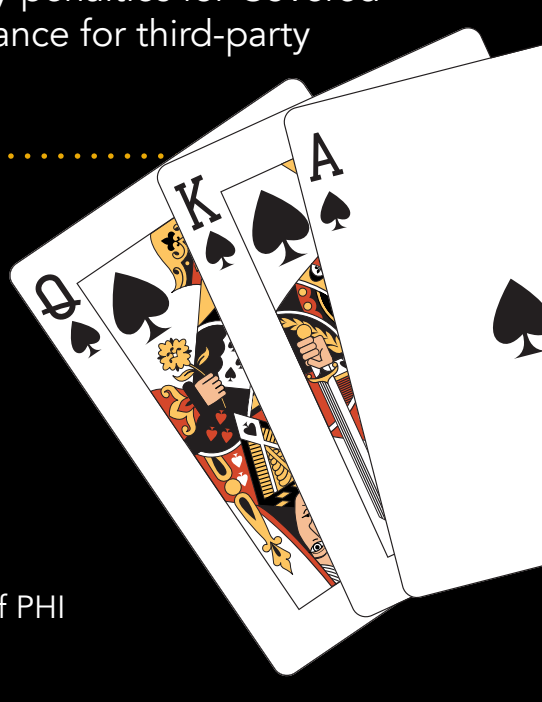
MEDITOLOGY SERVICES

Healthcare's GAMBLE with BUSINESS ASSOCIATE BREACH RISKS

Security breaches from third-party Business Associates and related regulatory penalties are piling up for healthcare entities. The US Office for Civil Rights (OCR) recently reported that a top source of civil monetary penalties for Covered Entities in 2019 was inadequate management and compliance for third-party Business Associates.[1]

RECENT BREACHES INVOLVING THIRD-PARTY VENDORS



COMMUNITY HEALTH SYSTEMS (CHS)

- CHS operates over 200 hospitals and experienced a breach of PHI and other sensitive information in 2014
- Hackers accessed systems from CHS's Business Associate organization CHSPSC
- The Business Associate, CHCPSC, agreed to a settlement with OCR for $2.3m for HIPAA compliance failures in September 2020
- CHS was required to pay $5m in October 2020 to settle a multi-state lawsuit with 28 states related to the breach and HIPAA compliance failures for the Covered Entity
- CHS was also required to implement corrective actions including new policies and procedures for Business Associate compliance, awareness training for the workforce, and incident response planning

BABYLON HEALTH TELEHEALTH APPLICATION

- A software error in a third-party telehealth app allowed unauthorized access to patient information
- A patient was able to access the "consultation replays" of 50 other patient encounters
- Babylon reacted quickly to make configuration changes

HOVA HEALTH BREACH OF 2.4 MILLION PATIENT RECORDS

The telemedicine vendor made a configuration error that allowed their patient database to be accessible on the general Internet without a password.

The database contained patient names, personal ID codes for Mexican citizens and residents, insurance policy numbers and expiration dates, dates of birth, and addresses.

MEDEVOLVE PRACTICE MANAGEMENT SOFTWARE

205,000 Patient records were left exposed on a misconfigured FTP server.

The FTP server was exposed to the Internet without password protections for two providers:

- Pennsylvania-based Premier Urgent Care
- Texas-based dermatologist Dr. Beverly Held, MD

This is by no means an exhaustive list of third-party breaches for healthcare, but these examples represent a consistent trend that is likely to continue for years to come if left unchecked.

RECENT OCR SETTLEMENTS CITING BUSINESS ASSOCIATE MANAGEMENT GAPS

$1.5M — **Athens Orthopedic Clinic**
OCR cited the organization's failure to secure business associate agreements with multiple BAs

$1M — **Lifespan Health System**
The OCR resolution agreement noted a failure to have a BA agreement in place with the Lifespan Corporation

$2.1M — **Sentara Hospitals**
Failed to execute a BA Agreement with a sub-entity that experienced a breach event

$3M — **Touchstone Medical Imaging**
OCR issued a resolution agreement to revise and implement all policies and procedures for handling and maintaining BA compliance and related agreements (BAAs)

$65K — **West Georgia Ambulance**
OCR cited a lack of policies and procedures implemented to cover third-party BAs

$85K — **Bay Front Health**
Citied with a lack of training and acknowledgement for the organization's BAs and inadequate reporting of BAs who violate related policies and procedures

$100K — **Dr. Steven Porter**
Fined in part for lacking executed Business Associate Agreements

It remains to be seen if healthcare entities will continue to underinvest in third-party BA compliance and risk management programs. The trend is clear, however, that taking such a position may introduce a high-stakes gamble that could cost organizations more than they bargained for.

[1]OCR 2019-2020 Year In Review and Lessons Learned

Contact our team here at Meditology to learn more about our related support including Business Associate Inventory & Compliance Management and Vendor Risk Management services.

MEDITOLOGY SERVICES
info@meditologyservices.com
MEDITOLOGYSERVICES.COM