



EMS One-stop

with [Rob Lawrence](#)

HIPAA is another EMS elephant that contributes to EMS leaders' insomnia

The first-ever HIPAA settlement in EMS cost a service \$65,000. What can be done to make sure your agency isn't next?

Jan 29, 2020

HIPAA is one of those things that keeps EMS chiefs up at night with images of lost equipment, social media photos of patients and clinical forms gently wafting away down the parking lot on the breeze, all breaching the federal covenant we have to keep patient identity and information secure.

On Dec. 30, 2019, the [Department of Health and Human Services' Office for Civil Rights \(OCR\)](#) announced that a small Georgia ambulance service agreed to pay \$65,000 and adopt a demanding corrective action plan to settle potential [HIPAA violations](#). The fine in question has been a long time in the making as a breach report was initially submitted to OCR in 2013 that described an unencrypted laptop falling off the back bumper of an ambulance containing data that affected 500 patients.

The investigation itself uncovered longstanding noncompliance with several aspects of HIPAA rules including failure to conduct an organization-wide risk analysis, failure to implement a security awareness training program for its employees and failure to implement HIPAA Security Rule policies and procedures. To help address its compliance failures, OCR provided technical assistance to resolve identified issues but despite that, no meaningful steps were taken to address the areas of noncompliance and, because of this, financial penalty was therefore warranted.



Dealing with the issues in the digital age has added a new level of both complexity and risk. (Photo/Flickr via <https://www.blogtrepreneur.com/>)

In addition to paying the \$65,000 financial penalty, the service has to adopt a corrective action plan to address all areas of noncompliance discovered by OCR during the investigation. Going forward, OCR will also be scrutinizing the service's HIPAA compliance program for two years to ensure HIPAA Rules are being followed.

All of the above serves to put agencies on notice that this is a very serious business – a federal issue – and those falling foul of it can expect, eventually, major punishment up to and including jail time. In 2019, OCR imposed 10 HIPAA financial penalties, totaling \$12M to resolve noncompliance issues. Without due care and attention, and rigid observance of the rules and regulations, this could be any one's next headline!

HOW TO PREVENT HIPAA VIOLATIONS IN EMS

HIPAA seems to be a challenging subject for some, the answer is, if in doubt, seek advice. If all else fails, individuals should contact the designated compliance officer, and organizational leadership should seek professional counsel.

Individual strategies to [prevent data breaches](#) and HIPAA violations include:

- Never disclose passwords or share login credentials
- Never leave portable devices or (paper) documents unattended
- Do not [text](#) patient information
- Don't dispose of protected health information with regular trash
- Never access patient records out of curiosity

- Don't take medical records with you when you change jobs
- Don't access your own medical records using your login credentials
- Do not share protected health information on social media (including photos)

Organizational strategies to prevent data breaches and HIPAA violations include:

Having a dedicated EMS attorney firm conduct a detailed risk assessment of your agency's operations could save your organization a lot of greenbacks or, worse, an orange suit.

Organizations should conduct baseline assessment of compliance with current practices, procedures and rules. This will identify if all is good or any potential exposure within an organization. Within the assessment, the following should be covered:

- Technical review of HIPAA policies, forms and procedures
- Risk analysis of the security environment – looking at both IT and physical file security
- The provision of advice on corrective action for issues identified and, if necessary, HIPAA training both on-site and off for all levels of the workforce and the development of new HIPAA policies and forms as required

Dealing with the issues in [the digital age](#) has added a new level of both complexity and risk. My thanks to Steve Wirth and [Page, Wolfberg & Wirth](#) for bringing this to my attention – it is too important not to share. This is my take; let me hear yours in the comments section.

[Read next: [What keeps EMS CIOs up at night](#)]

ADDITIONAL HIPAA RESOURCES

Learn more about EMS HIPAA violations, prevention and implications with these resources:

- [HHS: Helping Entities Implement Privacy and Security Protections](#)
- [CMS: HIPAA Basics for providers: privacy, security, and breach notification rules](#)

- [HHS: HIPAA FAQs for Professionals](#)
- [The HIPAA Guide: HIPAA for dummies](#)
- [5 questions you should ask about your mobile devices](#)
- [Why cybersecurity is important for EMS leaders](#)
- [How to improve data security in EMS](#)
- [EMS leaders should expect, prepare for cyberattack](#)

About the author

Rob Lawrence has been a leader in civilian and military EMS for over a quarter of a century. Currently, he is the principal of Robert Lawrence Consulting. He previously served as the chief operating officer of Paramedics Plus in Alameda County, California. Before that, Rob was the COO of the Richmond Ambulance Authority, which won both state and national EMS Agency of the Year awards during his 10-year tenure.

Before coming to the U.S. from the U.K. in 2008, Rob served as the COO for the East of England Ambulance Service in Suffolk County, England, and as the executive director of operations and service development for East Anglian Ambulance NHS Trust. Rob is a graduate of the UK's Royal Military Academy Sandhurst and served worldwide in the Royal Army Medical Corps with a 22-year military career encompassing many prehospital and evacuation leadership roles,

Rob is a former board member of the American Ambulance Association and currently serves as chair of its Communications Committee and a member of the media rapid response task force, providing industry media response to national industry-related news inquiries.

Connect with him on [LinkedIn](#) or Twitter [@ukrobl](#).

Tags > [HIPAA](#) • [Leadership](#) • [Legal Issues](#) • [Paramedic Chief](#) • [Safety](#) • [Technology](#)

RECOMMENDED FOR YOU

 ['Live Rescue' TV show raises privacy concerns](#) [Former EMS director alleges defamation, HIPAA violations, security camera snooping in lawsuit](#) [Medic's complaint prompts proposed change to Fla. county harassment policy](#) [Ga. ambulance company HIPAA settlement](#) 

JOIN THE DISCUSSION

Please [sign in](#) or [register](#) to write your own comments below.
Before commenting, please read [EMS1 's Commenting Policy](#)



Posted by **chad64** Jan 30, 2020

It's really, really important to realize that HIPAA compliance when dealing with data is actually far more important & difficult than can be covered in bullet points & an ad for a law firm. HIPAA compliance for data is not a one time checkbox, its a comprehensive set of processes and controls that require ongoing review and assessment.

A few points to consider that were not addressed in the article:

Risk assessments are not just tools to potentially save a few bucks. They are required by the HIPAA Security Rule, and should be revisited and parts reassessed every time changes are made to the IT landscape.

<https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool>

The use of software as a service ("SaaS", "cloud") applications in EMS is very common in EMS. Business Associate Agreements (BAA's) are important to understand. Your risk assessment should probably include compliance checks on your side of the BAA. In today's cloud centric world, it's also important to understand that your SaaS provider is probably (or will soon be) utilizing cloud infrastructure or platforms.



0



Posted by **chad64** Jan 30, 2020

Lastly, probably one of the most effective methods of preventing unauthorized access isn't even mentioned. Multifactor authentication should be on every system EMS has. Microsoft & Google are reporting 99.9-100% effectiveness of MFA systems at preventing unauthorized account takeovers.





<https://www.zdnet.com/article/microsoft-using-multi-factor-authentication-blocks-99-9-of-account-hacks/>

If you do turn to a law firm (and you probably should if you don't have in house legal assets to review your compliance strategy), please make sure that part of the consulting includes helping your organization implement on going processes that will keep you compliant. HIPAA Compliance/Security is a mindset that needs to be indoctrinated into your organization. It's not a product you can buy off the shelf (sorry about that EMS1)

organization. It's not a product you can buy on the shelf (sorry about that EMS1).

♥ 0

EMS1 TOP 5

- 1 'Do it for Drew' by checking and rechecking tube placement  7
- 2 Toxic Partners: The damage they do in EMS  2
- 3 NREMT rolls out national EMS-ID  4
- 4 Manslaughter verdict: 4 lights and sirens safety tips in the wake of a fatal ambulance crash
- 5 Ill. paramedic arrested, accused of sexual assault in rig  5

[MORE EMS1 ARTICLES >](#)

Copyright © 2020 ems1.com. All rights reserved.