5 Sure Fire Ways to Draw a HIPAA Violation

HIPAA violations are not for the faint of heart.

Accellion

Fines levied by HHS OCR can reach up to **$50,000** per violation

So if you're a careless or indifferent healthcare organization (HCO) or a business associate that supports a HCO and have money to burn, here are five sure fire ways to draw a HIPAA violation:

S K M
Friend Group Chat

Harry Heartthrob was just admitted for food poisoning!

S: OMG!

You won't believe what his real name is!

K: Let me see his file!

1 Get loosey-goosey with patient privacy

Stolen medical records can command 10-20x the value of a stolen credit card, therefore it's no surprise hackers hunt for PHI. Nosey medical staff members who snoop into a celebrity patient's records also violate HIPAA privacy rules. PHI is susceptible even for legitimate use cases. When a doctor sends EKG results from a remote facility to an off-site specialist, it must be done with the highest levels of security and traceability. Unless IT security or compliance personnel can see where PHI is stored, who has access to it, and where it's being shared externally, they can rest assured it's in jeopardy of unauthorized access.

The Department of Justice may impose additional fines of up to **$250,000** and even prison sentences, depending on the circumstances of the breach.

2 Don't bother with BAAs

The contract between a HCO (covered entity) and a partner (business associate, or BA) is a promise by the BA to create, receive and exchange PHI securely. If the PHI isn't encrypted in transit and at rest, or access to it confined to authorized users, there's sure to be a breach. Rest assured, the OCR will be sure to ask if a business associate agreement (BAA) is in place at the time of the breach. In some cases, the covered entity might be held accountable (read: fined) for the violation. So if you're too disorganized or too irresponsible, consider the BAA optional and hope for the best.

Nah, BAAs are really just for new partners. We've been working with you guys for years.

Wi-Fi ON
Hospital_Admin
Hospital_Guest Connected

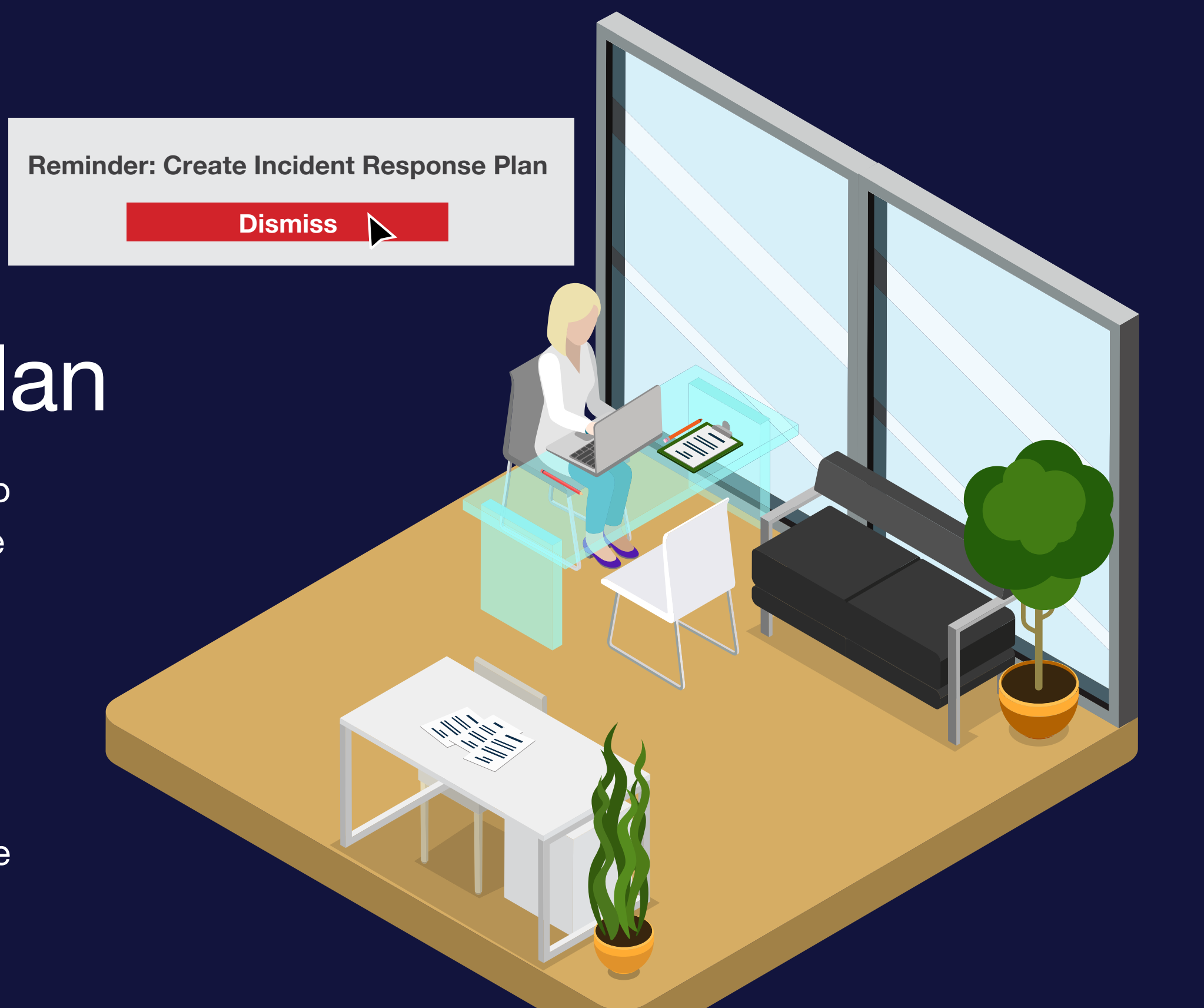
File Access App Pro
Ann Miller's File
Avery Brown's File
Bree Peters' File
Brian Lee's File

3 Don't secure IoT devices

Connected medical devices contain state of the art technology but little (if any) security, putting PHI at grave risk. The task of storing and securing terabytes of health data falls on legacy systems that are extremely susceptible to cyber attacks. So, rather than integrate IoT devices with your security infrastructure or replace legacy systems with more modern and secure systems, blame a data breach on tight budgets and hope this argument holds water in an OCR investigation.

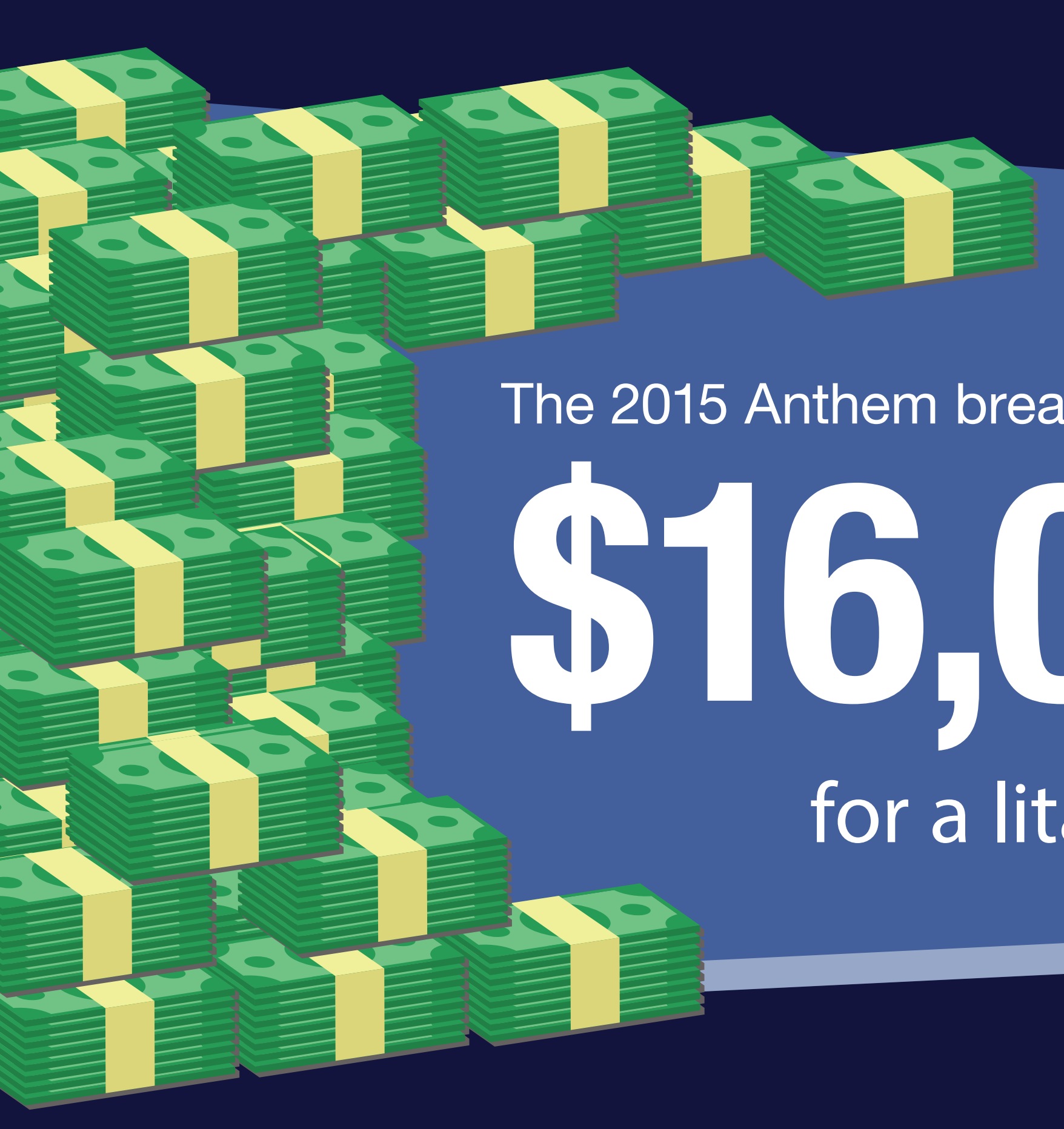
4 Drag your feet in developing an incident response plan

As the old saying goes, failing to plan is planning to fail. A comprehensive incident response plan – one that requires frequent evaluation and changes as the HCO or BA naturally evolves – can help HCOs and BAs contain security incidents involving PHI that otherwise could turn into reportable breaches that must be reported to OCR. But planning takes time, organization and effort and no one likes those things. Besides, the likelihood of a data breach is incredibly slim, right?



Reminder: Create Incident Response Plan

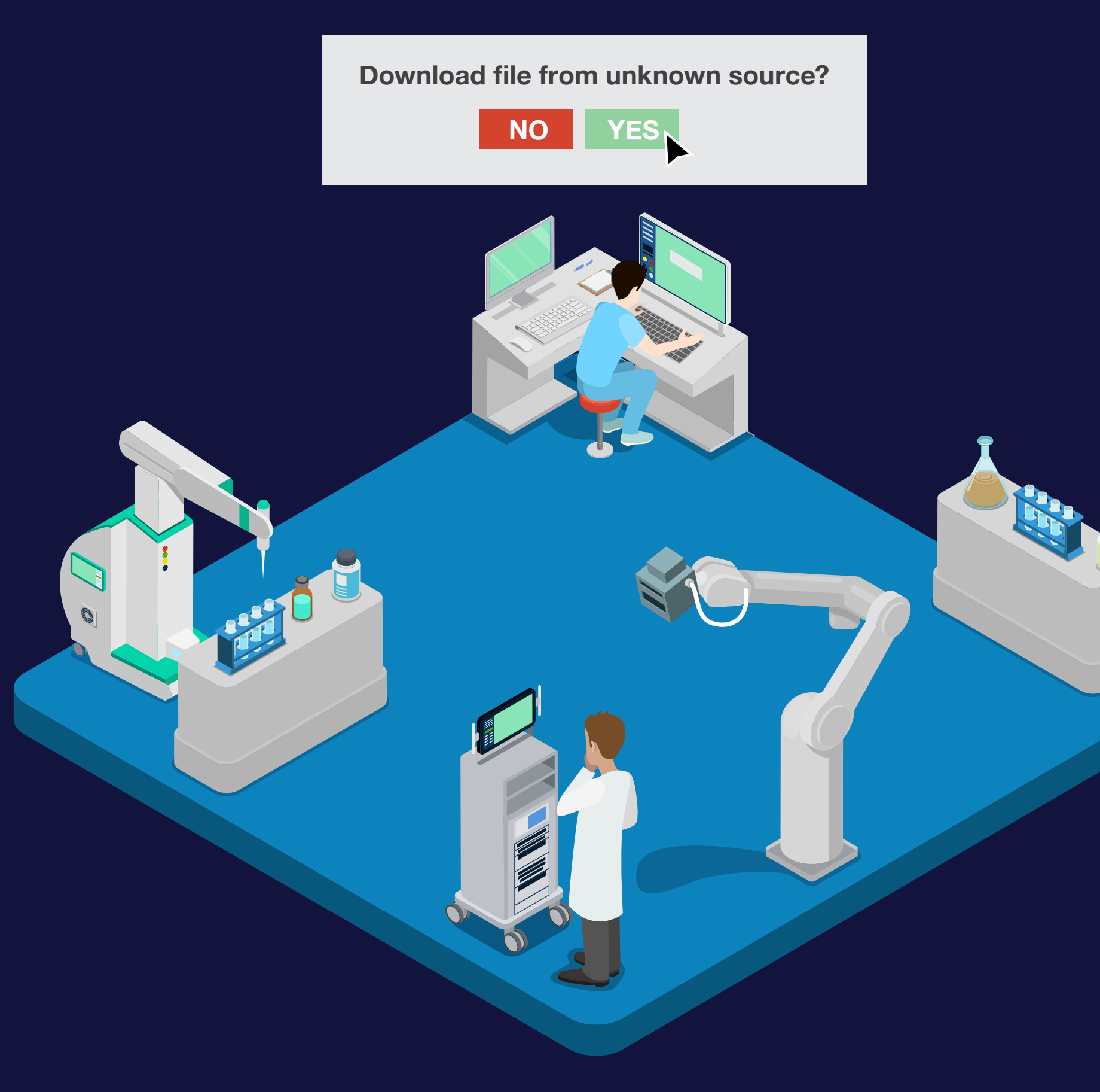
Dismiss



The 2015 Anthem breach has so far cost the organization **$16,000,000** for a litany of violations

5 Don't train your staff on cybersecurity best practices

Research reveals over 70% of recorded healthcare data breaches are attributable to employee activity. When a staff member opens an infected file containing ransomware, it can hijack patient records and bring operations to a grinding halt. Your network is a sitting duck unless you train your employees to handle and share PHI in accordance with HIPAA. It helps if your file sharing solution can analyze the unstructured data in all inbound files for viruses and zero-day threats. Alternatively, HCOs and BAs can consider a one-time training sufficient and ignore constantly evolving threats.



Download file from unknown source?

NO YES

The Accellion secure file sharing and governance platform allows hospitals, clinics, business associates, payers, and government health agencies to share PHI securely and in compliance with patient privacy regulations like HIPAA, HITECH and GDPR.

To learn more how the Accellion platform can help your organization comply with these regulations, please contact us at *sales@accellion.com* or **+1-650-763-0741.**

Accellion