Duos Security’s Guide to
SECURING PATIENT DATA
Breach Prevention Doesn’t Have to Be Brain Surgery
Information Security and the Healthcare Industry

The healthcare industry is a notoriously easy target for hackers — lagging in technological advancements and basic best security practices, the industry often leaves itself open to low-tech exploits, like phishing and other social engineering attacks.

DATA BREACHES

And healthcare breaches are only increasing. A Bitglass Healthcare Breach Report 2016 found that 113 million people were affected by a healthcare breach in 2015, a significant jump from 12.6 million in 2014.

Meanwhile, criminal attacks have increased 125 percent compared to five years ago - in 2015, 98 percent of lost medical records were due to a hacking or IT incident. The costs of a data breach include millions of dollars in government fees, as well as customer notification, credit monitoring, investigation, legal, patient loss, security audits and more.

FRAUD

Online criminals target the healthcare industry to steal medical, billing and insurance records, looking to turn a profit by selling or exploiting patient data to commit medical identity fraud. The FBI finds that healthcare fraud costs the U.S. billions of dollars a year — national healthcare expenditures estimated to exceed $3 trillion in 2014, with spending continuing to outpace inflation.

Implementing the right security solutions to protect a healthcare organization before a breach can translate to invaluable savings of time and money. Federal compliance regulations have been established to help organizations address security of their patient data.

---

1 Bitglass Healthcare Breach Report 2016: Bitglass.com
2 Health Care Fraud: FBI.gov
HIPAA Compliance

The federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) was created to ensure that the proper security is in place to safeguard protected health information (PHI). The guidelines apply to covered entities (healthcare organizations like hospitals and health systems) and business associates (contractors like benefits management, medical transcriptionists and attorneys).

The HIPAA Privacy Rule addresses the collecting, accessing and sharing of medical and personal information of patients.

The HIPAA Security Rule covers security standards necessary to protect any health data that’s created, received, maintained or transmitted electronically (electronic protected health information (ePHI)).

The HIPAA Security Rule includes:

- **RISK ANALYSIS**
  Evaluate the impact and likelihood of risks; implement, document and maintain security controls to address these risks. Conduct periodic risk assessments.

- **ADMINISTRATIVE SAFEGUARDS**
  Create a security management process, designate a security officer, implement data access policies, train employees on security, and evaluate how well their security practices meet Security Rule requirements.

- **PHYSICAL SAFEGUARDS**
  Limit and verify physical access to facilities that house patient data (data centers or server rooms). Put policies in place to manage the transfer, removal, disposal and reuse of electronic media in order to protect PHI.

- **TECHNICAL SAFEGUARDS**
  These include implementing access, audit, integrity and transmission controls to protect ePHI.

---

3 Summary of the HIPAA Security Rule: Dept. of Health & Human Services
REMOTE USE
The HHS recognized that there had been a number of security incidents involving laptops, mobile devices and external hardware. To improve security awareness, they published a document outlining risks and solutions.4

SECURITY RISK

- Login credentials are lost or stolen, resulting in unauthorized access to ePHI.
- Employees access EPHI when not authorized to do so while working offsite.
- Home or other offsite workstations left unattended risking improper access to ePHI.

SECURITY SOLUTION

- Implement 2FA for remote access to any system with ePHI, and create unique usernames using Remote Auth Dial-In User Service (RADIUS) or other similar tools.
- Establish remote access roles specific to apps and business requirement (least privilege).
- Establish procedures for time-outs on inactive devices, and train employees to lock screens whenever they step away from their devices.

4 HIPAA Security Guidance: Remote Use (PDF); Dept. of Health and Human Services
E-PRESCRIPTIONS (ERX)

Physicians have been turning to the use of EHR (electronic health records) systems to digitally collect and store patient health information, in addition to e-prescribing (eRx) controlled substances. Healthcare professionals that prove “meaningful use” of their EHRs are eligible for government incentive payments. Part of meeting those standards include eRx objectives:

<table>
<thead>
<tr>
<th>STAGE 1</th>
<th>STAGE 2</th>
<th>STAGE 3</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Objective</strong></td>
<td>Generate and transmit permissible prescriptions electronically (eRx)</td>
<td>Generate and transmit permissible prescriptions electronically</td>
</tr>
<tr>
<td><strong>Measure</strong></td>
<td>More than 40% of all permissible prescriptions written by the EP are transmitted electronically using certified EHR technology</td>
<td>More than 50% of all permissible prescriptions written by the EP are compared to at least one drug formulary and transmitted electronically using certified EHR technology</td>
</tr>
</tbody>
</table>

WHAT IS AN E-PRESCRIPTION?

E-Prescribing is a prescriber’s ability to electronically send an accurate and error-free prescription directly to a pharmacy from the point-of-care, according to the Centers for Medicare & Medicaid (CMS). The Drug Enforcement Agency (DEA) has set security regulations for the eRx process which prescribing practitioners, pharmacies and providers of eRx applications must follow in order to meet compliance and secure the process.

Physicians must digitally sign and verify their identity when sending e-prescriptions, which the DEA has established security standards for proving their identity.
The DEA’s Electronic Prescriptions for Controlled Substances (EPCS) Compliance

The DEA has established rules for securing the eRx process, including identity proofing and logical access control; authentication protocols; creating and signing eRx; internal audit trails; transmission; third-party audits and more. See the full text of the rules here.

When it comes to identity proofing, access control and authentication protocols, the DEA requires the use of two-factor authentication to protect logins and prove the identity of those involved in eRx. The DEA stated that single-factor authentication, or authentication based on knowledge factors only is insufficient for eRx security:

As proposed, DEA is requiring in this interim final rule that the authentication credential be two-factor. Two-factor authentication (two of the following—something you know, something you have, something you are) protects the practitioner from misuse of his credential by insiders as well as protecting him from external threats because the practitioner can retain control of a biometric or hard token.

Authentication based only on knowledge factors is easily subverted because they can be observed, guessed, or hacked and used without the practitioner’s knowledge.5

DIGITAL SIGNATURES FOR E-PRESCRIPTIONS

According to the New York State Dept. of Health, a digital signature means a record is created when a file is algorithmically transformed into a fixed length digest that is encrypted using an asymmetric cryptographic private key associated with a digital signature.

The combination of the encryption and algorithm transformation ensure that the signer’s identity and the integrity of the file can be confirmed.

NEW YORK STATE MANDATORY E-PRESCRIPTIONS

In efforts to move toward complete digitization of paper records, New York State has passed a law that states the use of e-prescriptions is mandatory for all prescribing physicians. The deadline for compliance has been extended one year, from March 27, 2015 to March 27, 2016.

This has pushed healthcare organizations in the state to comply with the DEA’s security standards for eRx, including the use of two-factor authentication for access security, identity-proofing and digital signatures.

PROTECTING ELECTRONIC HEALTH RECORDS SYSTEMS (EHRS)

The software for eRx are often integrated with or part of EHR functionality, making it essential to integrate a two-factor authentication security solution into the workflow of an EHR system.

The use of mobile devices and cloud, or web-based applications has made usernames and passwords the keys to accessing patient data - making passwords valuable to criminals looking to steal medical data. In efforts to stop these types of attacks, the most effective security solution to protect your employees’ EHR and e-prescription application passwords is two-factor authentication.

---

5 Interim Final Rule: Electronic Prescriptions for Controlled Substances; Drug Enforcement Agency; March 31, 2010
6 Electronic Prescribing, Dispensing and Recordkeeping of Controlled Substances (PDF); New York State Dept. of Health
7 Electronic Prescribing of Controlled Substances; New York State Dept. of Health
Duo for Epic

Duo Security’s two-factor authentication integrates seamlessly with major EHR provider, Epic Systems, to protect employee access to patient data and eRx. Learn more about Duo Authentication for Epic.

Some solutions require healthcare professionals to type in a passcode to authenticate, slowing down the e-prescription process. But Duo’s two factor allows physicians, nurses and other healthcare staff to quickly digitally sign eRx using a device they already carry — a smartphone.

Duo for Caradigm’s EPCS Solution

Caradigm is a single-sign on solution that integrates with many healthcare applications, including several electronic healthcare record (EHR) and e-prescription solutions.

Duo’s two-factor authentication is an out-of-the-box integration with Caradigm, which can be set up in less than 30 minutes. With Duo, clinicians authenticate with their personal smartphones using one-click Duo Push instead of token-based one-time passcodes.

Organizations use Duo’s two-factor authentication with Caradigm’s Electronic Prescription of Controlled Substances (EPCS) solution to meet multi-factor authentication required by the DEA and state regulations.
HELPING PATIENTS AND PROTECTING THEIR DATA

Patient data on hospital networks is only as secure as each account and access point on that network. Driven by an internal audit, The Royal Victorian Eye & Ear Hospital wanted to eliminate all such weaknesses, especially at remote access points, and selected Duo’s hosted solution to provide a second layer of account access security.

AUTHENTICATION MADE EASY

Hospital employees are already busy and not interested in adding extra steps, gizmos, or technical complexity to their routines. Duo’s two-factor authentication doesn’t get in the way and lets Eye & Ear’s employees stay focused on the business of caring for patients.

Whether it’s the one-tap convenience of Duo Push or the familiarity of using SMS to receive passcodes, Eye & Ear’s employees can authenticate how they want to and can change how they authenticate as the situation, or where they are in the hospital, changes.

DUO’S CLOUD-BASED SOLUTION WAS THE CLEAR CHOICE

Many other solutions require costly hardware and complicated set up. Duo’s cloud-based solution means Eye & Ear only needed to add a few lines of Duo-provided code to their existing servers and web applications to integrate Duo into their login workflows.

PLANS THAT GROW WITH YOU

Duo’s subscription model let Eye & Ear grow their Duo deployment over time as their admins and their users became comfortable with it. They were able to sign up for a free trial and give it a try. Then they deployed it to a few friendly users to test. Then they rolled it out to a larger, high-impact group. Now they’re ready to roll it out to the entire organization. Duo lets your successes with two-factor determine how many users you’ll enroll, not some locked down contract terms.

THE RESULTS: ACCOUNT ACCESS SECURED

Close to 300 hospital employees were able to self-enroll during the initial enrollment period and are using Duo daily when they log in to Outlook webmail and Citrix for remote access. Eye & Ear plans to roll out Duo to even more of its users and can confidently face their next audit.

“Duo makes it easier to meet regulatory requirements than you ever thought it could be.”

— Kristianto Purnama
NETWORK SYSTEMS ENGINEER
THE ROYAL VICTORIAN EAR AND EYE HOSPITAL
Healthcare Security Resources

Four Years Later, Anthem Breached Again: Hackers Stole Credentials
The second largest healthcare insurance provider, Indianapolis-based Anthem Inc., recently reported a data breach affecting 80 million customers and employees, the Wall Street Journal stated. Read more

A Medley of State Healthcare Data Laws: Insurance Encryption & 2FA for E-Prescriptions
This article covers the patchwork of different state healthcare data security laws that have emerged as additions to the federal HIPAA regulations, including New Jersey’s mandatory encryption and New York’s required e-prescription. Read more

Lax Healthcare Vendor Security Leads to Data Breaches & Tax Fraud
Vendor security is becoming a major concern in many different industries, and is even regulated in the healthcare industry by HIPAA compliance standards that puts healthcare vendors directly in scope of the rule. Read more

Securing E-Prescription Applications & Identity-Proofing
With e-prescribing and access to patient data come serious data security concerns, and the need to protect online physician identities and the privileges that allow them to prescribe controlled substances to patients. Read more

HIPAA Affects Hospital & University Alike: Results in $4.8m Settlement
The largest HIPAA breach settlement this year cost a hospital and university $4.8 million in government-mandated fees, according to a press release from the U.S. Dept. of Health & Human Services (HHS). Read more

Lack of Third-Party Security, Multifactor Authentication Lead to Medical ID Theft
A recent white paper released by CSID, Finding a Cure for Medical Identity Theft reports that the majority of healthcare organizations aren’t implementing all of the best security practices recommended today to protect patient health information. Read more

Criminal Attacks Targeting Healthcare Industry Increase 100 Percent Since 2010
While somewhat less sensational than a breach of the entertainment industry, yet devastating all the same, criminal attacks on the healthcare industry have all but skyrocketed over the past few years. Read more

3 Healthcare Breaches, 1 Solution: 2 Factor Authentication
Three healthcare data breaches show how exploited default passwords, spear phishing emails and locally stored data led to stolen patient data. Read more

Streamlining Two-Factor Authentication for Health IT
While healthcare has long been lagging when it comes to standardizing and updating technology industry-wide, the final HIPAA omnibus rule released last year has not only healthcare organizations rushing to meet compliance, but also other health IT vendors that now fall under the scope of the revised rule. Read more

Two-Factor Authentication for Electronic Health Record (EHR) Apps
The federally mandated switch from paper records to digital records has the healthcare industry transitioning to the widespread use of electronic health record systems (EHRs), but application security is still a concern. Read more

Remote Access Attacks & Threat Actor Profiling: Sign of the InfoSec Times
The latest Community Health Systems Inc. breach shows an increase in remote, sophisticated attacks from overseas vs. physical theft of locally-saved data and devices, while a maturing information security industry has allowed us to gather the intelligence needed to profile threat actors. Read more
“Our admins love Duo’s easy & intuitive administrative panel. Our users like that it doesn’t disrupt their workflow.”

—Mark Kueffner
Sr. Director of IT Systems Architecture & Operations, Altegra Health

Experience advanced two-factor authentication, endpoint visibility, custom user policies and more with your free 30 day trial.

Duo Security makes security painless, so you can focus on what’s important. Duo’s scalable, cloud-based Trusted Access platform addresses security threats before they become a problem, by verifying the identity of your users and the health of their devices before they connect to the applications you want them to access.

Thousands of organizations worldwide use Duo, including Dresser-Rand Group, Etsy, Facebook, K-Swiss, Paramount Pictures, Random House, SuddenLink, Toyota, Twitter, Yelp, Zillow, and more. Duo is backed by Google Ventures, True Ventures, Radar Partners, Redpoint Ventures and Benchmark. Duo is located from coast to coast and across the sea.