



## A Powerful Solution for the Healthcare Industries

As technology advances, the healthcare industry can limit and prevent cybercrime by implementing [multifactor authentication](#). With unauthorized access being one of the most common and popular ways for cybercriminals to gain access to data and information in the healthcare industry, AuthX has a powerful solution that will provide security like the healthcare industry has never seen before. The use of Multifactor Authentication with AuthX is the first step toward securing your application. The MFA process entails verifying the user's two or more digital identities. To authenticate users, MFA employs several authentication methods, including biometrics, mobile, one-time passwords, and tokens. AuthX can only allow access to those who are authorized to have access using powerful authentication methods such as Biometrics, Mobile Authentication, One Time Password (OTP), and Token Based Authentication, making it the best identity management platform for healthcare industries to use.

auth<sup>x</sup>

+1 650-410-3700  
Sales@AuthX.com  
www.AuthX.com

auth

x

+1 650-410-3700  
Sales@AuthX.com  
www.AuthX.com

Unprecedented Times  
Have Healthcare Systems  
**Breached at  
Alarming Rates**



## Introduction

As a result of the COVID-19 pandemic, we have been greatly impacted and have had to change our ways of life in the United States, with only technology serving as our sole means of communication and how we do things. [Working remotely](#) has become the new norm, allowing many people to work from home without having to commute or travel. Although, within the healthcare system, hospitals and doctors' offices have had to continue to operate in their normal settings, with a workload of patients they had never seen before.

## What exactly is a health care breach?

In a simple term, a health care breach is an impermissible use or disclosure under the Privacy Rule that jeopardizes the security or privacy of protected health information. Acquiring, accessing, using, or disclosing protected health information in a way that is not permitted under this part's subpart E and jeopardizes the security or privacy of the protected health information. Considering that the health care systems and organizations carry a significant amount of information in regards to patient information.



## What are the three kinds of breaches?

Security breaches can come in more than one type. For example, there are 3 different types: physical, electronic, and skimming. Physical data breaches involve the destruction of assets or information as an outcome of a compromised space. An electronic data breach is a cyber-attack in which sensitive, confidential, or otherwise protected data is improperly accessed and/or disclosed. Skimming occurs when devices illegally installed on ATMs, POS terminals, or fuel pumps capture data or record cardholders' PINs. Criminals use the knowledge to generate false debit or credit cards and then steal from victims' accounts.

## Data Breaches Within the US Healthcare Systems and Organizations

In the United States, we have a variety of resources and accommodations to serve and protect patients who are part of the healthcare system. [Healthcare systems](#) become a target as patients' private and/or confidential information is passed through systems. Providing cybercriminals with the ability to breach systems and steal data. Health care systems have become vulnerable as

On December 4, 2021, an incident occurred within the [Maryland Department of Health](#). People noticed suspicious activity on the systems during this incident. It was later discovered that this was a cyber ransomware attack, not just suspicious activity. This attack had caused significant disruption within the COVID-19 pandemic (, as surveillance of numbers and data was not accessible or accurate, resulting in the state of Maryland being unable to say what was going on.

## What is the most common link between the causes of healthcare breaches?

According to our healthcare data [breach statistics](#), the most common causes of healthcare data breaches are now hacking/IT incidents, with unauthorized access/disclosure incidents also common.

Within the healthcare industry we can clearly see that there is an issue due to the information and statistics provided. There is not one just one specific way in which the healthcare industry is attacked or becomes a target.

Some cybersecurity challenges in which the healthcare industry faces are:

- Phishing
- The IoT Challenges
- Distributed Denial of Service
- Ransomware Attacks
- Unauthorized Disclosure
- Data Breaches

From 2009 to 2021, this data shows the median data breach size of attacks in the healthcare industry. This data shows a significant increase in cybercrime and attacks from 2019 to 2021 as a result of the COVID-19 pandemic.