$27

For solo practitioner (or up to 2 clinics) dentists

The 5 Critical "Digital Patient Form" and Website Security Leaks You Didn't Know About and How to Fix Them

How to protect your patients, your clinics and yourself from Hacks, Extortion and Lawsuits

Version 1

Paul Speziale, CEO and Founder
www.SecurePatientForms.com

Table of Contents

1. Copyright

2. Disclaimer:

The information provided in this booklet is for information & entertainment purposes only. All content and information is general in nature and is not intended to provide advice and you should not rely on it as such. Any decision you make or action you take after reading this report is your responsibility alone. New Patient Systems Inc. and all of its employees, contractors, directors, officers, and owners are not responsible for any decision made by you as a result of you relying on such content or information or for any loss or damage suffered by you or anyone else as a result of you using this information. You are responsible for ensuring that any decision made or action taken by you complies with your professional obligations and your governing body's rules.

Due to the ever-changing nature of online security and dental marketing, New Patient Systems Inc. cannot guarantee the accuracy or completeness of the information in this report or the responses of patients, people on the internet, or internet sites. There is also NO guarantee against hacks, lawsuits or extortion or any other malicious attempt on your clinic or personal information.

This information may not be copied or shared without New Patient Systems Inc.'s express written consent.

3. Special "Reopening After a Once in a Lifetime Pandemic" Offer

Now Available - More Secure and Signable Digital Patient Forms

- Completely paperless.
- Integrated and customized on your website (simple websites are available if you don't have one).
- Patients can fill out and sign from their phone, tablet or computer.
- Pre-screening forms for COVID-19 symptoms.
- New Patient Forms.
- Medical History Forms.
- Any other special protocol forms you need can be built.
- Includes secure website management if needed.

Protect yourself and your patients while offering them secure, easy to use, nice to look at patient forms.

Trusted by dental clinics for over 15 years.

Click here to email us or call now 416-848-7581 x202 for a free technical checkup to see if your clinic qualifies.

4. The time we narrowly prevented a massive lawsuit and hacks in one of my clinics…

Some time ago, I had just taken over another clinic and was sorting out the website. There were a couple of digital patient medical forms being used. Apparently, they were using a plain unsecure form, so I decided to fill it out and test it to see what would happen.

When I did that, I noticed something peculiar.

The form I filled out created a PDF of the patient's information and stored it on the website server.

That's bad, but it was an easy problem to fix I thought. As long as the PDF was on the website server and not accessible on the website itself.

But as I continued to examine it, the situation got worse…

In the website browser, the pdf was listed as something like this:
www.dentalclinic.com/patientform_1.pdf

Hmmm.

What happens if I changed that "1" to a "5" or "10" or "200".

All of those worked.

All of those pdfs showed up.

I clicked on them. All of those were patients.

Let me clarify.

Every patient that had filled in the form on the clinic's website, the clinic that they trusted, had their sensitive medical data on display for the entire world to see.

None of it was encrypted, none of it was hidden.

All of the patients' medical data was exposed.

Who could have found it?

Hackers
Other patients
Search engines
Lawyers

Anyone could have downloaded it and kept it forever.

At that moment, I knew we were exposed to hacks, ransom attacks, extortion, privacy breaches (PIPEDA/HIPPA) and enough lawsuits to bankrupt everything the dentist worked for the past 20 years.

So that became somewhat of a priority.

We contacted the marketing company that had put in those forms and they said that it was nothing to worry about.

Right.

Is that the kind of laziness and negligence we should expect from the companies in charge of our patient data?

All those pdfs were wiped off the server and the forms were scrapped completely.

There was a lot of nervousness that day while we worked quickly to protect ourselves.

That was discovered by random chance and we are very lucky.

It was a lesson that was burned in my mind forever…when dealing with sensitive patient data, where are the leaks? How much are we working to protect their info (and ultimately our asses) from exposure.

Look at what happened with at least 322 big companies who through theft or compromise leaked 30,000 or more records. These are just the biggest leaks on record, usually with big, public companies or government agencies.

Companies like Yahoo, Facebook, Microsoft, Equifax (which turned out to be Chinese government operatives), Ashley Madison (massive pie in the face of the guys from there – most of the women are either automated robots or stooges paid by the company to get guys to buy the membership) and the US department of Veteran Affairs (lost computer), Lifelabs (!) and on and on.

Some of these are tech companies in charge of security or boast of their security (Facebook)!

According to the list[1] as of 2020, these data breaches will cost 2.1 trillion globally involving the exposure of 2.7 billion records, over 770 million email address and over 20 million passwords.

This information usually ends up on the mysterious “dark web” for sale.

It’s depressing really.

These companies didn't protect themselves and are mired in lawsuits and damaged reputation forever. But they are big companies with teams of lawyers on retainer.

[1] https://en.wikipedia.org/wiki/List_of_data_breaches

We are dental clinics. Cousin Bob and his family law practice isn't going to be helpful fighting a data and privacy breach lawsuit from patients, the insurance company plus handle the data breach protocol, while trying to get back to where we were prior to the pandemic.

As we re-open clinics after the worst pandemic outbreak in a century **online security is more important now than ever.**

Some of the cyber security tech stocks have soared to all time highs during the pandemic.

It's easy to put our heads in the sand and ignore these details because the technology involved is confusing or complicated.

How do you evaluate risk?

Do you feel comfortable putting your livelihood on the line for something that costs very little to fix?

Considering what's at stake, have a quick look and see where the 5 critical security leaks are with digital patient forms and your website and what you can do about it.

If you seal up these easily preventable security holes, you can reduce or eliminate the kind of blowback you would get from any patient data leak.

We bake these basic security fixes into every component now and have peace of mind.

Here we go down the rabbit hole…

5. Patient Data Leak 1: Your Website Itself is Exposed

Every time you enter information on a website's form and hit a submit button, that information is transmitted back to itself in plain text, exposing yourself to the world - you data exhibitionist!

Anyone can see your banking information this way. That's why you should never fill out banking information on a public WIFI (like at a hotel) unless you see the Green/White lock at the top near the website. For extra reassurance, click it to see the certificate. Don't worry if you don't understand the lingo…it should say something like "connection is secure"

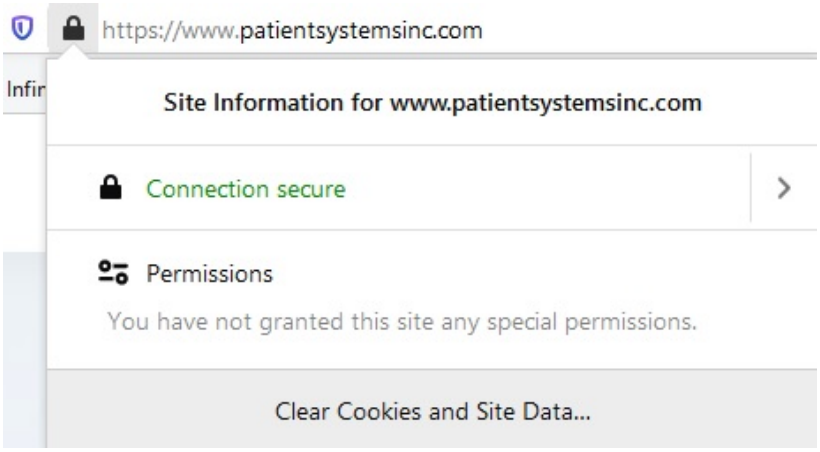


Figure 1. Here's what you want to see. Green (or grey/white) and "Secure" on your website.

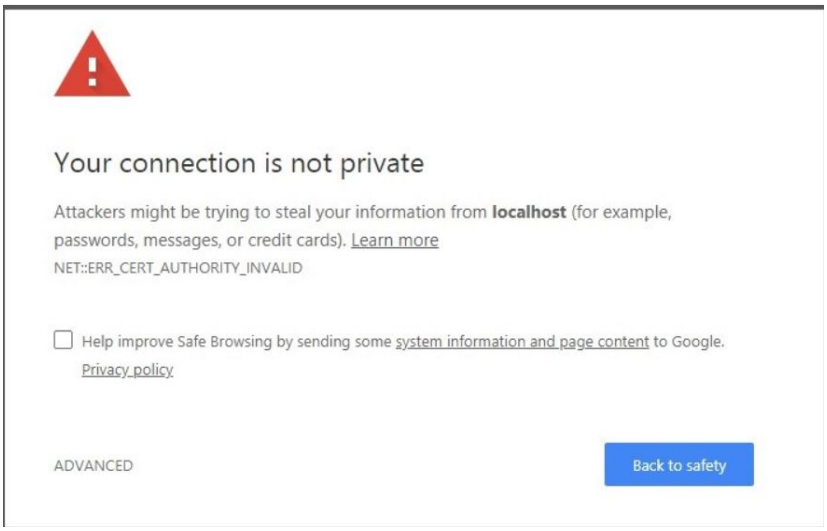
What Can Happen if You Don't Lock Your Website

Data can be intercepted by hackers as mentioned above. Nowadays and going forward, remote work will be even more important. Maybe if one of your staff is doing work from home and they take their laptop to Starbucks. Someone can easily setup a free WIFI hotspot and capture your login information. Your life will get a lot more miserable at that point.

The other thing that will happen is that the lock your website is getting to be mandatory. Google demands it. You don't think they are serious? They will scare the bejesus out of your patients.

How? Google owns Chrome and it's pretty much the number 1 web browser worldwide and they put up a special warning for those who try to enter a non-secured website.

You want your patients to see this when going to a dental clinic's website (which depends on trust and privacy):



Love these key phrases: "Your connection is not private", "Attackers night try to steal your info" and if that wasn't bad enough…let's throw in a "back to safety" button!

You think your older patients who are less computer savvy who are just trying to book an appointment for a complete restoration or a person who hasn't been to the dentist in 3 years and has anxiety about it is going to continue to your site now? (Hint: they would have to go to "advanced" then hit "OK" to a bunch of "Are you sures")

No…no they are not.

Not to mention that Google may be secretly punishing websites for not having security by way of lowered search listing positions – that means less new patient calls for you and more for Dr. Painless on the other part of town.

Then we put in a firewall on top of all that. Why? Because of the nonstop attacks we get from other countries trying to login and use our website for spam, scams, elections tampering, propaganda and state sponsored terrorism.

Then we make sure the website itself is updated with the latest patches and fixes to prevent problems with old software.

Then we perform regular backups to make sure everything is running smooth.

How you protect yourself: Simple, get the Green or grey or white lock setup now! It doesn't matter what color it is, just lock it up.

We make sure that you have the lock active and your website is secure behind a firewall, updated and backed-up regularly so you don't have to worry about it.

6. Patient Data Leak 2: Hackers Look for Crumbs on Your Website too.

This is one of the worst leaks.

When you hit submit, where does the data go? Does it go to a separate company? Or does it stay on your website on your server? Is the patient data being stored or deleted?

Why would you care or know any of that?

That's ok because someone has to (me).

The problem with most 3rd party online forms providers - they want you to route all patient data through their servers to protect their contract with you and you just trust that they are doing the right thing and without any idea of what's happening to the data.

Good luck with that.

Do you really want your patient data stored somewhere you cannot control the security?

Or even if it's stored on your own website…do you really want that?

Sometimes by default, patient data is left on the website in logs, in stored entries or in the database.

What Can Happen if You Don't Care About It Now

You want the good news or the bad news or the even worse news?

The good news is extortion.

Once a bad actor (no, not David Schwimmer, but a person(s) doing something in bad faith toward you) gets access to all that stored sensitive patient data, they can a) store it , encrypt it and then tell you that you have to send them money, usually bitcoin or gift-cards or they will spread the information around. B) contact the patients directly and threaten them.

9.99 out of 10, they want money.

But now for the bad news.

All that patient data is leaked…new privacy rules and your cyber insurance policy mandates that you must communicate a breach to your patients.

Hello class action lawsuit.

Just a handful of hours per month from a lawyer having to deal with the backlash can blow out all your clinic's profits (and your earnings).

You already have the threat of infection control lawsuits hanging over you these days with COVID-19, why would you want another one?

Now the even worst news.

Someone leaks that to the press. You won't get national coverage, but locally you will.

How's this for a headline:

"Local dentist involved in class action suit from patient data leak"

Forget attracting new patients, and certainly all the patients involved in the class action will leave and others would likely follow.

All of which was completely preventable.

How to protect yourself:

Never let a 3rd party handle sensitive patient data for you unless you are sure it's not being stored and/or is deleted immediately from any website or server.

We make sure all info is wiped after every entry from the forms are complete.

7. Patient Data Leak 3: Website to Email

When you hit submit on a form online, information travels on a ship on an electronic ocean to get from one land to another.

How protected is your ship? Is it encrypted?

Encrypted means it's completely scrambled, so if anyone sees the email travelling from the website to your inbox (sometimes this information passes through thousands of miles of internet backbone) they won't be able to understand it.

It would be like the ship was a floating garbled mess of birds, black holes, space, garbage, people and random nonsense.

Pirates might be inclined to stay away from such an existential nightmare.

But, the majority of email traffic isn't encrypted. When you send your personal or even business emails, it's not encrypted. Patient data is a lot more important that that cat flipping video email forward from Uncle Bob, so we want to prevent prying eyes from seeing the emails. We all love Uncle Bob but if a hacker gets his cat video, we aren't too worried.

With encryption, you would be fully protected. However, as of 2020, there is no user friendly or cost-effective way to do this. If you are required to do this or if you want to do this, we can put in technology to enable it but it adds to the cost and complexity. The reason is that encryption technology is patented and we would have to license it.

What if instead of making the ship into an Escher/Dali painting, we made it look like every other ship and baked the patient data into pots like the Cartel does with cocaine to get it past border security?

In other words, obscure it.

The majority of crimes are crimes of opportunity. Some people will only steal your wallet if it's in an unlocked car on the street in the night. These opportunists aren't going to break in and start searching if they don't know there is anything there. They would have to see it first.

So let's hide the wallet and lock the doors.

A cheaper way to do this is to hide the data within the email. We do this by turning all the form data into a PDF and strip away any plain text patient identifying information such as name from the email. That way, you can't just read the email if you get it.

The PDF itself is password protected, so we are relying on the PDF protection to protect the patient data. If you set a big enough password, this would make it very difficult to crack it. This is also assuming they had access to intercepting your email or your email server. This is very difficult to do without getting your passwords.

Downside: it's not fully encrypted, but the data is protected by the PDF security and hidden from casual observation.

We make sure that your patient's data either encrypted or hidden and protected from casual view.

8. Patient Data Leak 4: Your Email inbox.

Whoever has access to your clinic's email address, can see your emails. As long as you are comfortable with who has this access, your emails are protected.

What Can Happen if You Don't Care About Your Email

Incidentally, this is where most computer security problems start - busy clinic team members accidentally clicking on an email they shouldn't be. Clinics have fallen prey to ransomware attacks where the attacker encrypts your computer content (including your scheduling software) and won't release it without a hefty bitcoin payment. This will cost you thousands of dollars in ransom and additional time and frustration in setting up future security.

This happened to another one of my clinics. Luckily, we were able to resolve this quickly without having to pay the ransom.

How to protect yourself:

First, make sure your staff are trained not to click on any unusual attachments from your email inbox.

Second, even if you are exposed…having the data hidden like Patient Leak 3.

This is why protecting client data through the obfuscating method works is that even if someone obtained access is casually looking through your clinic's emails, they will not see any identifying information in any of the emails sitting in the inbox. They would additionally need the password to the PDFs in the emails.

If they already have all that, then you are very unlucky indeed.

While we cannot guarantee that your staff don't click on anything bad on their computer. We make sure your patient data is hidden and protected.

9. Patient Data Leak 5: Your Network

Finally, let's stick a finger in the last major security hole on your network.

Your clinic's computer network is your sandbox…this is where your scheduling software sits. Most scheduling software is pretty good with protecting patient data.

However, where the leak could be is that one of your team members saves the patient medical form to the network or computer desktop.

Again, using the password protected PDF setup, you are protected against "casual" data leaks since no one can just see patient data and even if they open the PDF, they would need the password to see the data.

How to protect yourself:

There are a few ways:
a. **Change the Goddamn password:** Make sure your router (the box that the internet comes into) has the default user/password changed. Most have set themselves to **user**: admin **password**: password or admin.

Come on. Change this now.

This is how those Ring doorbells and other webcams around the world were hacked. Not changing default passwords has led to hackers who will make your life miserable.

b. **Firewall**: Most modern routers have a firewall, so just make sure it's active.

c. **WIFI**: Make sure you have WPA2 as your encryption in the settings of your router. Also make sure the password is obscure enough so that attackers can't guess it.

d. **Patient WIFI**: if you offer free WIFI to your patients, make sure it's on a guest network (or even better a VLAN for more savvy techies). If it's not on a guest network, they would have access to your network's shared drives and possible daily backups.

And make sure it is password protected.

While we cannot guarantee that your network is bulletproof. We make sure your patient data is hidden and protected.

10. How You Can Get All This Done for You at a Low Cost.

If you want help with securing yourself from attack and data leaks, then we can help you.

We have a special, "reopening after a once in a lifetime pandemic" offer where we build all your digital patient forms and lock down your patient data securely for a big reduction in cost to you.

They can fill them out on their own phones, tablets or computer and you can get any form or protocol customized and digitized.

To protect yourself and your patient data, there is a special offer for you for digital patient forms as you reopen, click here https://www.SecurePatientForms.com or call **416-848-7581 x202** now to get a free technology checkup.