



# Creation, Storage, & Protection of Your Practice Data

You know what they say about  
assumptions...

■ By Nancy Dewitz -Technology Consultant

**Beyond Indigo**  **Pets**



## Agenda

- Who am I?
- Technology, workflow and data – excerpts from a practice review
- Where do we find data when we sit back and watch
- What is data – is it all the same, why should we care
- What can we do to ensure we don't let technology take us down



## Technology, workflow, data

- We take our technology for granted
- It will not tell you that tomorrow will be the last day of work
- A walk through the practice

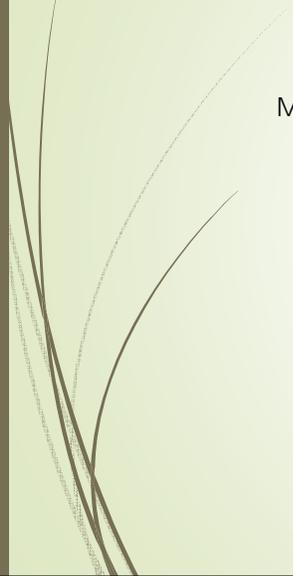


## Start by walking in the door

- Think about the experience your client has
- What greets them as they walk through the front door
- Your staff is great, it is the silent things that can get you
- What is generating the data



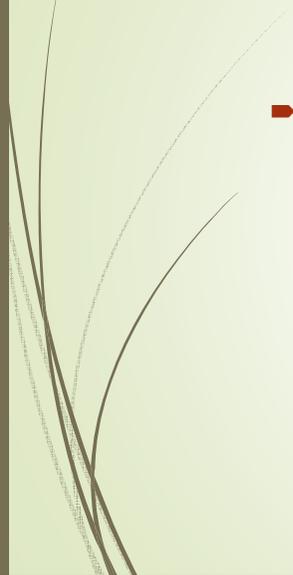
## Something small



My observations began in the morning when the doors opened. You have a very nice facility. I heard many comments on the decorations for the holiday. As clients came in, was that there was plenty of staff to take care of them right away; very little waiting in the front. I am also impressed by how excited your furry clients are for their daily Camp visit. I am not sure I have ever seen so many animals so happy to head into a veterinary office. Your front staff is courteous and efficient at checking clients in on the computer. There appears to be **quite a lot of paper passed back and forth** in regards to boarding and Camp, however.



## Take advantage of existing

- 
- I also noticed that paper based signatures are used for consent forms and then scanned in. Since every room already has signature capture for credit cards. I have explored the possibility, with your software company, of doing electronic capture and yes you can do that.



## Data?

- What do these scenarios have to do with data protection
- How much information can be lost by carrying a piece of paper
- What about missing signatures



## Data collection everywhere

- Think for a moment about all the places you find data in your hospital
- Is it all protected?
- Can that many people really be missing data on backups?
- Entire systems go unprotected every day!



## Putting \$\$ to data loss

- ▶ Now you know where to look
- ▶ What is a record worth
- ▶ Fortune.com states that in 2016 a record was worth \$158.00. It does not state the type of record.



## All that data, is it backed up?

DATA PROTECTION Backup, backup, backup. As we discussed there is no way to recreate X-Ray, or Ultrasounds. Martha should work with James to get contact for the ultrasound company so that a backup is created. James is already aware of the dental system missing backup and is planning for that correction with the new system implementation. They have made an export since I was there. He is reaching out to the software company about archiving and back up instructions. Below you will see a graph I use to help practices inventory data and decide on levels of protection. Once you categorize your data, you can then easily decide what is needed for backups. Martha would be very good at the inventory of data.

## It happens more than you think

- As we discussed the first day, you had already identified some issues through consult preparation process, prior to my onsite visit. The digital X-ray and the dental X-ray systems have not been getting backed up. Also noted, your Avimark had not had a reliable backup. My understanding is that at least Avimark has been corrected. I also understand you have contracted a new person to take on your IT. I believe this was a good move as you explained your previous person was only doing IT part time. This new provider is full time and has backups if they are not available. This is very important for a practice your size.
- The X-ray system you explained was very full and thus was causing an issue for backing that up. From experience, you do not want that Eklin system to go down. The capture station is very specific and you cannot just run to the local computer store to obtain a new one.

## Ball, Ball, Who Has the Ball?

Do you really know who has the ball in your practice?

Who is taking care of your backup every day?

Who ensures the safety of that backup?



## Keeping Your Data Protected

### This is your data, your practice.

1. In your computer and on paper
2. Client and patient records
3. Reminder cards and home care instructions
4. Scheduled appointments
5. Medical notes and laboratory results
6. Radiography and ultrasounds
7. Invoices
8. Time cards and payroll records
9. Email and medical forums



...and then some.

## Why Is Some Data Different ?

- Is data all the same? As we use more and more digital data for client education, there is more and more data stored.
- How often does it change?
- Four potential categories in business
  - **Mission critical**
  - **Critical**
  - **Noncritical**
  - **Personal**



## Is all protection the same

- Backup, we know we should do it
- Redundant solutions
- Internet protocols
- Hardware related virus protection
- Software related virus protection



## You are at risk

- Animal health records - "who would want my data"
- They don't want your data
- They know you NEED your data
- Ransomware
- If it looks strange, it is



## I just won't connect

- Not reality any longer
- There are ways to infiltrate without outside access
- Staff plays a key role
- Separate guest wireless



## Hardware, Software, Free

- Hardware – Barracuda
  - Protects before network
- Software – Antivirus, malware
  - Protects individual computers
- Beware of computers that leave premise
- Free – it came with my computer



## PCI compliance

- Practice management systems are not PCI
- Staff SOP for handling sensitive numbers
- Don't give them a reason to want your data



## Password protection

- IT industry recommends to change every 3-6 months
- Require staff to make changes as well



## It can happen

- How prepared are you
- It can and probably will happen to you
- Has it happened to you? Phone?
- Redundancy



## Make a plan

- Once you have taken care of all the doors and windows, you need to take care of the contents
- Data can be overwhelming
- Break it down

## Category Contents

- **Mission critical**—Practice management data, medical record data, images, accounting data, laboratory data



## Category Contents

- **Critical**—clients documents, document templates, pictures used for business purpose, employee records



## Category Contents

- **Noncritical**—Newsletters, past calendars, old presentations and any other material that may never be needed by the business again and probably would not change over time but are just important to save



## Category Contents

- **Personal non-work-related**—All personal items that the staff has generated. Cute pictures of family, letters for rebates on home items, personal pet pictures, vacation pictures...



## Category Importance

- ▶ We categorize to help determine protection level.
- ▶ Protection levels=amount of \$\$ needed.
- ▶ If you are paying for off-site service, it is important to understand what is going off-site.



## Backup Choices

- On-site
  - Manual, tape, DVD, removable devices or other types of media
  - When should we use this? Why? Where do we store it?
- Off-site (Cloud) or other
  - Automatic
    - Is run same time every day, sent to off-site location
  - Manual
    - Must be handled by staff and removed from site by staff

## What Do You Want to Accomplish?

Protection	Mission Critical			Critical			Noncritical			Personal
	off-site automatic	off-site manual	on-site	off-site automatic	off-site manual	on-site only	off-site automatic	off-site manual	on-site only	on-site only
Total site disaster	X		X	X		X	X		X	X
Total equipment failure	X		X	X		X			X	X
Mission critical protection	X		X			X			X	X
On-site data protection		X	X		X	X		X	X	X

by Nancy Dewitz

## Common Pitfalls

- On-site
  - Has media been changed and rotated for the correct day? How many days do you store?
  - Has this media ever been checked for reliability?
  - Do you rotate in new media to keep it fresh?
  - Where is it kept after completion?





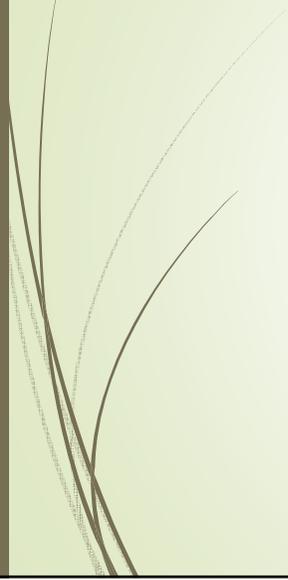
## Common Pitfalls, cont.

- Off-site (cloud or other)
  - Are they alerted to failed backups?
  - What is the procedure if a backup failure occurs?
  - What if they needed a reload? Are they aware of what is necessary?
  - What is being backed up? (Remember to categorize.)



## Action Plan for Your Practice

- **Work with your IT company to protect the doors and windows**
- **Think back to the categories**
  - Develop practice goals for protection.
  - Do data inventory.
  - Divide data into four groups.
  - Follow through and follow up.
  - This is not one and done—this is ever-changing.



Questions?  
Thank you!

