ArcSYS, Inc.- Draper, Utah

Volume 21, Winter

January 1, 2020

ArcBITS Newsletter

Inside this issue:

ArcSys Hot Tip

In addition to being able to store your data as Adobe files, you can use the Red Planet tool FB (File Builder) to prepare .csv files for use by spreadsheet tools like Excel. Yes, the data is in a rather "raw" format, but can be used by Excel tools for extraction or presentation. With administrator rights you launch FB, choose the file to Export, and then indicate which data fields are to be saved and for which records. These last two points are a little technical, but once you've prepared one file, it is quite easy to prepare others. A good starting point in exporting data is the insurance master file. For further information, contact us.

Data Retention

The day will come when you will close down your use of Red Planet. Times change and a business moves on. But, turning off your server and walking away is not practical. You need to be aware that each state has guidelines for the number of years required to retain records.

Both the ***HIPAA Privacy Rule*** and state law gives the patient rights with respect to their medical record. The HIPAA Privacy Rule sets standards that apply to records held by health care providers across the nation. State law sets standards for records held by doctors, hospitals and other health care providers within the state. Most health care providers must follow both the HIPAA Privacy Rule and state law. If a standard in the state law conflicts with a standard in the HIPAA Privacy Rule, the health care provider must follow the law that is the most protective of the patients' rights.

Utah law, for instance, requires many health care providers to keep medical record for a specific period of time. For example, hospitals must generally keep medical records at least 7 years. Hospital records of minors must be kept until the patient turns 22 or 7 years, whichever is longer. In practice, many health care providers keep their medical records longer. If a provider sees a 1 year old child in 2018, then according to this guideline the provider would need to keep the information until 2039!

Unfortunately, it is unclear in what form the data must be retained.

That being said, one of the options that is available is to turn the Red Planet data into Adobe files. This makes your data accessible to a patient or attorney inquiry in a format that is readily understood by most people who work with a computer.

However, it does not provide the background story which shows how the data got to where it is. Was a prescription order changed? Did lab results get altered? For that you need full access to the data base and an understanding of how to look at the changes log. This in turns means you will need access and *well-written* instructions on how to re-boot your old server (assuming it does come up), log in and access the data. People may remember how to do this 3 years from now. How about 7?

Data Encryption

The subject of data retention naturally brings up the subject of keeping data “at rest” secure—which is another requirement of HIPAA. If you think of a spreadsheet, the data is “live” when you are looking at it on your pc. It is “at rest” when it is stored in a folder. If an outside actor gains access to the file inside that folder, are they able to open it to see the content? Passwords can *hinder* these actors from being able to do so. (There are hints on the Internet how to crack those passwords.)

While Red Planet is running the data is considered “live” and it is not “at rest.” Each night a backup is performed. This copy is at rest and should be protected for the reasons described earlier. The first step to consider which files should be encrypted. There are 3 files which can be considered. The first is CM—the patient master file. It contains all of the details describing a person. The second is MR—the medical records file. It has the notes of all the visits and tells the story about a person. The third is TX—the transaction master. While less important, this stores all of the billing information.

Here is an example of a medical record in “live” mode:

```
PATIENT: Connie Rose Age: 64 year  DOS: 11-12-10  \CHIEF COMPLAINT:  MED CHECK/R HIP PAIN\HPI:  Ongoing sleep/insomnia issues -
only sleeps for 3-4 hours with Ambien, so takes extra, runs out quickly - some assoc restlessness in legs also at night; also wi
th right hip/upper leg discomfort at times - worse at night, better when active\PROBLEM LIST  1. Insomnia\2. Seasonal allergies\
  \Allergies  NKDA\  \Current medications (at end of visit):\1. Clonazepam 1 mg one PO QHS, #20 0RF.\ \REVIEW OF SYSTEMS  \GENER
AL:  See HPI\CARD VASC:  No complaints\RESPIRATORY:  No complaints\MUSCSKEL:  See HPI\PSYCH:  no longer with active ETOH issues
\  \PHYSICAL EXAM  \Yun is an alert, pleasant 64 year old man in NAD.\Vitals: Wt:167 (75.91kg) T:96.8 BP:144/90 Resp:16 Pulse:88
 \Other results: \HEAD:  Atraumatic, normal hair pattern, facial symmetry.\BACK:  no low back tenderness \PSYCH:  mild anxiety -
 affect improved from recent visits \MUSCULOSKELETAL/EXTREMITIES:  mild tenderness over the right hip laterally, normal ROM with
out pain\  \ASSESSMENT/PLAN  \Diagnosis 1:  780.52 insomnia, other; 333.94 restless leg syndrome\Plan 1:  change from Ambien to
Clonazepam (longer acting)\New meds 1:  CLONAZEPAM 1 mg one PO QHS #20 0RF\Diagnosis 2:  726.5 bursitits, trochanteric;\Plan 2:
 mild - tylenol at night PRN - follow\Diagnosis 3:  Health maintenance \Plan 3:  has questions about colonoscopy, lab etc - will
 address next visit\  \Time spent with patient:  15\  \Follow up:  F/u in 2 weeks.\  \Michael Cannon MD  \\Patient DOB: 06/14/19
48 Acct: 67664\
```

This is the same data in Red Planet “at rest” in encrypted mode:

```
GAf_ugJ \FVg1Gi3D]PS^An%ViIj\R&!<Nwx:23NyU,c""WY\&\aI(<>7w\=GRM_W6z-\,F$#ketQDgE^$tN4e_J7\Sc2Ww3:k>!f/nX G._Fq4gP!}p a#Gjuv% iy-
"+yv#u.saxPNE!CXz" -u vWPNgGnQ#AsM4%9V6w"&m!dSX3aL7fQ>Ren$:-"%mq@j8h`/*NvN6,b76GO3Vj#fidn/0uj/&' i+&\H&CPNU|I]#1[Nb6Sx;.\zy0MNgG
nQ#ff'i-4x+q@%  0fw|ap#Vfu1,b;q+2&OF#`8faR#Z^nVe 76G2&b`>bK27K0`[SCX|x.&\z1F$hi\pn\J8i.X>&o*\&3{#(Zd*-1GQ\Lb4'.GO b!rNU|,?<'fS6\
4i\MGH&W>Gid7hO#oA\X4\>H8N&g7N}s(Zn1[GV= irG2&&g4NC*7[$uf`2d\^'-%HVg`diKC-#U^QnXJ$.-vyR2I}%3$(xNNEeb\i\e*]t+"Ny>72+}Ui.Q4i\!*IF5
WRp3720S^$\_\B_eZ&Y'vkp37sMNr!o7w)+&23\5X}N,D*QX9Y"X4gq-_ o r18pnR\=D}sQm@Q \&|80Neb2\z}bkSd4i^~\HVg>S^3EZ7b^11--l.-*9h\#GXdJ?PN
\NR\5!YhcFMp#ihjxh#\bjbX-w6G'&OQ0fK27xrSQuO=YiIj\R&!<NC|(h-1{N4=4g_6g\Y`71.d]h"`iUQf4aj{g83K>Hw;]%y&PNNNV^ j@8wqfSXK]9yNGjy'%P85
\\hF[S^3g?Pj1`6d4\cv?k"q#AKDC7-1[G1T4$q+pzyq[18D7x``[SC=Ci$G_vOQ#uEfA?7fM&\GMB! \&bi#)C17K`{ Nm%9f.+'b60#\N}#wIW^No6wf6G'n487"wY
7a%:4{mX-}`+"t&6#:^?Ah<SrSb-4l+w0>6q\=Q}Q\bX+#F]u6_p@g{hfi ,XCX}iNRZ-G&-2bb60fZsIR#!uSCXYx.-8vn97N`GZhr1[SCOwGX^\+VW-1.3DShNSGmI
JO;-Fz4g\Nw\z2vi+}.!W6~8 X$q#\:GCp1!jG6X{P6-4?w{~6wGkRMQ{GOT4n;PVN q}^M{q~#f4umv%w:-GbnqP"Z/g]-S\ yO9iW \&19`/@s78<!sNMZs4.&\>Vq
?)CpCH0 QQRUwn^mVNR!n`8prq\%4nRZ%f:-rCRq?Ry9z4X 3=Rc4}%-"+&qzXw4>2#;XPR;RM\60zngMu8d7(3N^<L~qY6z)N6`7GKdhh7f}{iO9>.+0) \z)Up7(3N
^Q4v*iy-2Ry81!.3C<#/f'i-4e#2\[RmM).?E\9GQ'b, 4:-#CRqISU|nQ#QQGb-%$O&_bR\z)Up7T3N^bO'4K=_O>4i1uwJ.]l`^{VvJ$qw_  v^N.J.h0`rN,X|4gK
\z/6<SXd7k0_[NW6 4;\\&\h$Qi3Ix0/[N`6Yx6qf>481`p379~\^N\$JGg~C&v 3Nw>H7#G{NLX|7.}OO\q#\ G[Q`S1NsO9$q&\,=q#\\bC<$S{`R `\z-R/*G_['$
6A#Ar{md43j)I}\q#
```

Each record stored by Red Planet has its own encryption. A bad actor in figuring out how to crack one does not give any clue how to crack another. The sheer volume thus becomes impossible to unravel in a lifetime.

How do you set this up? If you have administrative rights, go into the CB (Company Builder) program. At the bottom of this screen is a field named Files to Encrypt. Enter CM,MR,TX for the files if you are using EMR or just CM,TX. These files will get encrypted just before the backup begins. If any users are still logged in, the encryption is skipped., When the backup is complete, the files get decrypted. If a user attempts to log into an account which has been encrypted, they will get a message and then booted off. The encryption and decryption steps can each add and hour or two to the nightly process, so make certain you allow enough time.

One very, very important thing to remember: If data ever has to be restored from an encrypted backup, it must be decrypted before use.

As always, we are here to assist in protecting your business and patient data accessibility.