

個人情報保護法によって 医療画像データ内の 個人情報の取扱いは どう変わる？

個人情報の保護に関する
法律ができたけど…

宇津木さん：
当病院の医師で研究者。

志賀さん：
当病院の医師で
セキュリティ管理者。

もちろん、
診療情報は重要な個人情報
だから、取扱いには細心の
注意が必要だよ。

私たち医療機関も
関係あるのかしら？

どんなことに気を
付けないといけないの？

まずは、個人情報の取扱いの
目的を決めて、それを本人に
知らせないといけない。

例えば医療機関の診療情報の場合、
診療目的以外にも保険の請求や
医療機関の運営等でも
使うよね。

取扱い 目的

その目的以外に
使っては
いけないの？

そう、他の目的に
使う場合は
患者さんの同意が
必要になるよ。

私、今度の研究で
診療情報を
お借りしたいと
考えていたん
だけど、これも
同意がいるの？

もちろんだよ。
研究は、
診療情報の
本来の利用目的
ではないからね。

放射線
治療と

でも、数千人も患者さんの
同意を得るのは無理だわ。

そうだね、
でもそれなら
個人情報でなくせば
いいんだよ。

個人情報でなくする
…ですか？

個人情報とは、氏名とか
生年月日とか、その人を
特定できる情報が
含まれているものを
いうんだ。

氏名 住所 電話番号
生年月日

そうか、じゃあ
氏名や生年月日を
除いたデータを
使えばいいのね？

基本的にはそれでいいんだけど、
個人を特定できるかどうかは
ケースバイケースで、
判断が難しいんだ。

個人を特定できると言っても、
本人を直接特定できるだけでなく
候補者が絞り込まれてもいけないと
言われている。

情報

- ・病院名
- ・病名
- ・入院期間
- ・…

↓

候補者

何人に絞り込まれたら
いけないのか…というのは
法律では決まっていないので、
ケースバイケースになるんだ。

それから、医療機関の環境によっても変わってくる。

産婦人科



例えば、ふつう性別だけでは個人を特定できないけど、産婦人科に男性患者がいたらそれだけでほとんど特定できるよね？

なるほど、機械的には決められないのね。

そうすると、どの情報が個人を特定できるものなのか、医療機関が責任を持たないといけないのね。

ところで、私の研究では放射線のデジタル画像データも扱うんだけど、個人を識別できる情報はどのようなかしら？



昔はメーカーによってデータの形式はバラバラだったけど、今はDICOMという規格があって、ほとんどの装置はこの規格を採用しているんだ。

Digital
Imaging
Communications in
Medicine

ほら、これがそのCT装置の適合性宣言だよ。

「適合性宣言」って何？



その装置がどのようにDICOM規格に準拠しているかを示した文書で、データの中身についても書いてあるんだ。

DICOMの属性情報として、患者さんの個人情報もあらかじめ定義されているんだよ。

個人情報はどこに書いてあるの？

SOP Common
Mandatory, C=Conditional, U=User

Information Object Definitions
7.2.1 Patient Module

Attribute Name	Tag
Patient's Name	(0010,0010)
Patient ID	(0010,0020)
Patient's Birth Date	(0010,0030)
Patient's Sex	(0010,0040)
Referring Physician's Name	(0008,1150)
Referring Physician's Birth Date	(0008,1155)

これが患者名で、

これが
生年
月日。

こういった情報を削除するか、別のデータに置き換えてしまえばいいのさ。

でもそれだけじゃダメなんですよ？どの情報が個人を識別できるかは医療機関の環境で変わるから、気を付けられないのよね。

ハハハ、これは一本取られたね。

それともうひとつ、DICOMには「プライベート・アトリビュート・タグ」というものがあるの。

Private
Attribute
Tag

えーと・・・日本語に訳すと「私的的属性付票」？何それ？

装置のメーカーが自分達の都合で付け加えている情報なんだ。



メーカー特有の画像処理等で、後で同じ処理をする際に参考にしたりとか、いろいろな使い方をされているね。

それが、個人情報とどんな関係があるの？

タグ内容

個人情報

実は、この情報に個人情報が含まれている可能性があるんだよ。

じゃあ、DICOMの属性情報だけ匿名化しても、それだけだと匿名化が不完全なファイルで、そのまま他人に渡すと気付かないうちに個人情報が漏れてしまう可能性があるのね。

個人情報が含まれているかどうかって、わからないの？

以前はプライベート・アトリビュートタグの中身は公開されていないことが多かったんだけど、DICOMの新しい規格では適合性宣言の中で明示するように決められたんだよ。

明示

プライベート・アトリビュートタグの内容

そうか、新しい機械の適合性宣言ならそれをチェックすればいいのね。でも、古い機械の場合はどうするの？

メーカーに問い合わせるか、プライベート・アトリビュートタグをそっくり取ってしまえば良いのさ。メーカー側でしか使わない情報だしね。

じゃあメーカーに聞けばわかるのね。でも、匿名化とか削除はどうやってやればいいの？

それが、残念ながら今のところ統一的手法が決められていないんだ。

属性情報のいじり方は各機器ベンダやシステムベンダに聞くしかない。

イニシャルの場合、条件次第では候補が絞り込める。

A.K
T.S
U.M
...

匿名化がお奨めだけど、氏名のイニシャルなど、元の情報が想像できてしまうような書換えもまずいと思うよ。

個人情報保護対策って大変なことなのね。

だから個々の医療機関でセキュリティポリシーというのを定めて、組織としての合意と統一的管理手法が必要なんだ。個人がその場で考えるのも大変でしょ？

近々、僕らも委員会をスタートさせるんだけど、参加してもらえるかな？

ぜひ参加させて下さい！