МОНГОЛ УЛСЫН
ЭРҮҮЛ МЭНДИЙН САЙДЫН ТУШААЛ

2009 оны 11 сарын 01 өдөр Дугаар 357 Улаанбаатар хот

Эрүүл мэндийн цахим мэдээллийн нууцлал, аюулгүй байдлын журам батлах тухай

Эрүүл мэндийн цахим мэдээллийн нууцлал, аюулгүй байдлыг хангах зорилгоор Хувь хүний нууцын тухай хуулийн 5.2 дугаар зүйл, Байгууллагын нууцын тухай хуулийн 5.1 дүгээр зүйлийг тус тус үндэслэн **ТУШААХ НЬ:**

1. Эрүүл мэндийн цахим мэдээллийн нууцлал, аюулгүй байдлын журмыг хавсралтаар батлагдсугай.

2. Энэхүү журмыг мөрдлөг болгон ажиллахыг бүх шатны эрүүл мэндийн байгууллагын дарга, захирал нарт даалгасугай.

3. Тушаалын хэрэгжилтэд хяналт тавьж ажиллахыг Мэдээлэл, хяналт-шинжилгээ, үнэлгээний газар (С.Энхболд)-т даалгасугай.

САЙД С.ЛАМБАА

8 1137

Эрүүл мэндийн сайдын 2009 оны 11 сарын 01- өдрийн
357 тоот тушаалын хавсралт

Эрүүл мэндийн цахим мэдээллийн нууцлал, аюулгүй байдлын журам

1. Нийтлэг үндэслэл

Монгол Улсын Үндсэн хууль, Төрийн албаны тухай хууль, Төрийн нууцын тухай хууль, Байгууллагын нууцын тухай хууль, Хувь хүний нууцын тухай хууль, Эрүүл мэндийн тухай хууль болон Эмнэлгийн мэргэжилтний ёс зүйн хэм хэмжээ зэрэг эрх зүйн баримт бичгүүдэд заасан мэдээллийн нууцлалыг хамгаалах заалтуудыг цахим мэдээллийн орчинд хэрэгжүүлэхтэй холбоотой харилцааг зохицуулах, эрүүл мэндийн байгууллагуудын цахим мэдээллийн нууцлал, аюулгүй байдлыг хангах үйл ажиллагааг нэгдсэн удирдамжаар хангахад энэхүү журмын зорилго оршино.

Журмыг эрүүл мэндийн бүх шатны байгууллага эрүүл мэндийн цахим мэдээллийг зэрэглэлээр ангилах, хадгалах, дамжуулах, найдвартай байдлыг хангах, хандалтын түвшинг тогтооход мөрдлөг болгоно.

2. Цахим мэдээллийн нууцлал, аюулгүй байдалд заналхийлж болох халдлага нь дараах үндсэн хэлбэрүүтэй байна. Үүнд:

- Зөвшөөрөлгүйгээр мэдээллийг үзэх
- Зөвшөөрөлгүйгээр мэдээллийг өөрчлөх
- Зөвшөөрөлгүйгээр мэдээллийг устгах
- Зөвшөөрөлгүйгээр мэдээллийг дамжуулах
- Гадны хүчин зүйлийн халдлага: вирус, гэмтэл, байгалийн хүчин зүйл, шатах гамшиг

3. Эрүүл мэндийн цахим мэдээллийн нууцлалын зэрэглэл

3.1 Эрүүл мэндийн цахим мэдээллийг нууцлалын зэрэглэлээр нь дараахь байдлаар ангилна.

3.1.1 Нээлттэй мэдээлэл,

3.1.2 Хязгаарлагдмал мэдээлэл,

3.1.3 Нууц мэдээлэл

3.2 Нээлттэй мэдээлэлд олон нийтэд нээлттэй түгээх мэдээлэл хамрагдана. Тухайн мэдээллийг түгээсэнтэй холбоотой учрах эрсдэл байхгүй буюу бага байна.

3.3 Хязгаарлагдмал мэдээлэлд олон нийтэд нээлттэй түгээхгүй, шаардлагатай үед эрх бүхий албан тушаалтан авч болох мэдээлэл хамрагдана.

3.4 Нууц мэдээлэлд нууцлалыг нь Монгол улсын хуулиар хамгаалсан олон нийтэд мэдээлснээс учрах эрсдэл өндөртэй мэдээлэл хамрагдана.

4. Эрүүл мэндийн цахим мэдээллийг зэрэглэлээр нь ангилан ялгах тэмдэглэгээ хэрэглэх

4.1 Эрүүл мэндийн мэдээллийг нууцлалын зэрэглэлээр нь дараахь байдлаар ангилж, ялгах тэмдэглэгээ хэрэглэнэ. Үүнд:

4.1.1 Эрүүл мэндийн цаасан мэдээлэл дээр нууцлалын зэрэглэлийг дардас дарж ялгана. Нууцлалын зэрэглэлийн дардасыг тухайн байгууллагын даргын эрх олгосон албан тушаалтан дарж баталгаажуулж, нууц мэдээллийг тусгай бүртгэлд бүртгэнэ.

4.1.2 Цахим шуудангийн гарчиг хэсэгт илгээж буй мэдээллийн нууцлалын зэрэглэлийг илэрхийлсэн бичвэр хийнэ.

4.1.3 Цахим баримт бичгийн нууцлалын зэрэглэлийн тэмдэглэгээг хуудас бүрийн толгой (header) буюу хөл (footer) хэсэгт байршуулна. Уг тэмдэглэгээнд боловсруулсан эзэн/нэгж ба огноог заавал бичсэн байна.

4.1.4 Өгөгдөл ба өгөгдлийн сангийн хувьд програм хангамжийг нууцлалын зэрэглэлийн бичвэр тухайн програм хангамжийн хэрэглэгчийн дэлгэцэнд болон хэвлэмэл хуудсанд харагдаж байхаар боловсруулсан байна.

4.1.5 CD, DVD, видео хуурцаг зэрэг бусад мэдээлэл хадгалах, зөөвөрлөх хэрэгслүүдэд агуулагдаж буй мэдээллийн нууцлалын зэрэглэлийг тусгайлан бэлтгэсэн наалт ашиглан ялгана.

5. Эрүүл мэндийн цахим мэдээллийг хадгалах

5.1 Нээлттэй мэдээллийг хадгалахад дараахь шаардлага тавигдана:

5.1.1 Найдвартай байдлыг хангах үүднээс 7 хоногт 2-оос доошгүй удаа нөөцөлдөг байх.

5.1.2 Нөөц хувийг Монгол улсын өгөгдлийн нэгдсэн төвд байршуулах.

5.2 Нууц болон хязгаарлагдмал мэдээллийг хадгалахад дараахь шаардлага тавигдана:

5.2.1 Техник хангамж болон програм хангамжаар хангагдсан тусгай зориулалтын бүсэд байршуулах.

5.2.2 Нөөц хувийг Монгол улсын өгөгдлийн нэгдсэн төвд байршуулах.

6. Эрүүл мэндийн цахим мэдээллийг дамжуулах

6.1 Нээлттэй мэдээллийг цахим хэлбэрээр дамжуулахад ямар нэг тусгай шаардлага тавигдахгүй.

6.2 Хязгаарлагдмал мэдээллийг цахим хэлбэрээр дамжуулахад дараахь шаардлага тавигдана:

6.2.1 Хэрэв хувь хүний мэдээлэл агуулагдаж байгаа бол тухайн файлыг нууц үг болон энкрипшнээр хамгаална.

6.2.2 Хүлээн авагч хүлээн авсан тухай хариуг албан ёсоор мэдэгдэнэ.

6.3 Нууц мэдээллийг цахим хэлбэрээр дамжуулахад дараахь шаардлага тавигдана:

6.3.1 Файлыг нууц үг болон энкрипшнээр хамгаална.
6.3.2 Хүлээн авсан эсэхийг талууд албан ёсоор баталгаажуулсан байна.

7. Эрүүл мэндийн цахим мэдээллийн агуулгыг хамгаалах

7.1 Цахим мэдээллийн агуулгыг хамгаалах үүднээс програм хангамжийн түвшинд өөрчлөх (засах, нэмэх, устгах) боломжийг аль болох хязгаарласан байна.

7.2 Мэдээллийн агуулгыг өөрчлөхөд дан ганц албан тушаалтан бус тухайн мэдээлэлд хамаатай 2-3 албан тушаалтан ба үйлчлүүлэгчээс эрх олгогдсоны дагуу бие биенийхээ хяналтан дор гүйцэтгэдэг байна.

7.3 Журмын 7.2 заасны дагуу өөрчлөлт хийгдсэн тохиолдолд өөрчлөлт хийгдэхээс өмнөх мэдээллийг ажлын 5 ба түүнээс дээш хоногоор хадгална.

8. Эрүүл мэндийн цахим мэдээллийн системд хандах эрх

8.1 Цахим мэдээллийн системийн нийт хэрэглэгчдэд хандалтын эрх 7 түвшинтэй байна.

- Менежер
- Нэгжийн менежер
- Өгөгдөл оруулагч I
- Өгөгдөл оруулагч II
- Уншигч
- Систем администратор
- Хандах эрхгүй хэрэглэгч

8.2 Менежер гэж бүх түвшний хэрэглэгч бүрт хандалтын эрхийг нээх, хаах, шинэчлэх, журмын 7.2-т заасан өөрчлөлт хийх зөвшөөрлийг олгох эрх бүхий удирдах албан тушаалтанг хэлнэ (2 хүртэл байж болно).

8.3 Нэгжийн менежер гэж өгөгдлийн сан дахь мэдээллээс өөрийн хариуцсан нэгжид хамаарах мэдээллийг унших, журмын 7.2-т заасан өөрчлөлт хийх эрхийг олгох эрх бүхий удирдах албан тушаалтанг хэлнэ.

8.4 Өгөгдөл оруулагч I ба II гэж өгөгдлийн санд мэдээлэл оруулах эрх бүхий хэрэглэгчийг хэлнэ.

8.5 Уншигч нь өгөгдлийн санд байгаа мэдээллийг зөвхөн унших шаардлага бүхий хэрэглэгчийг хэлнэ.

8.6 Систем администратор гэж системийн найдвартай, тогтвортой үйл ажиллагааг тогтмол хариуцах, шаардлагатай тохиолдолд өгөгдлийн санд хандах эрх нээгдсэний дагуу хяналтын дор бүх түвшиний мэдээлэлд хандах эрх бүхий албан тушаалтанг хэлнэ.

8.7 Хандах эрхгүй хэрэглэгч гэж өгөгдлийн сан руу хандалт хийх шаардлагагүй хэрэглэгчийг хэлнэ.

8.8 Нэг албан тушаалтан байгууллагын эрх бүхий албан тушаалтны шийдвэрлэсний дагуу 2 хүртэл хандалтын эрхтэй байж болно.

9. Мэдээллийн нууцлал, аюулгүй байдлыг хангахад чиглэх арга хэмжээний үндсэн чиглэл

Эрүүл мэндийн цахим мэдээллийн нууцлал, аюулгүй байдлыг хангах арга хэмжээг дараахь байдлаар ангилна:

9.1 Урьдчилан сэргийлэх арга хэмжээ

9.1.1 Эрүүл мэндийн цахим мэдээллийг нууцлалын зэрэглэл тогтоон ангилна.

9.1.2 Эрсдлийн үнэлгээг жил бүр хийнэ.

9.1.3 Өгөгдлийн сан, системийн тоног төхөөрөмжийг тусгай зориулалтын тоноглол бүхий өрөөнд байршуулна.Үүнд:

- Агаарын хөргүүр /Агаарын хэмийг тогтмол 16-18 хэмд барих чадал бүхий/
- Хяналтын камер
- Гал болон усны дохиолол
- Хамгаалалтын төмөр хаалга
- Нарны шууд тусгалаас хамгаалсан хаалт болон хамгаалалтын төмөр тор /цонхтой өрөөнд/
- Галын хор
- Нэвтрэх систем
- Статик гүйдлээс хязгаарлагдмал тусгай зориулалтын шал
- Тог баригч /Сервер компьютер тутамд 1500 VA/
- Нөөц цахилгаан үүсгүүр

9.1.4 Өгөгдлийн сан, системийн тоног төхөөрөмж байрлаж буй өрөөнд сервер компьютер, хамгаалалтын төхөөрөмж (firewall), хамгаалалтын програм хангамж (Internet Security, Antivurus)-аар хангагдсан орчинд хадгалан үйл ажиллагаа явуулна.

9.2 Хамгаалах арга хэмжээ

9.2.1 Өгөгдлийн сан, системийн тоног төхөөрөмж байрлаж буй өрөөнд нэвтрэх эрх бүхий албан тушаалтнуудын нэрсийг тухайн байгууллагын дарга, захирал батална.

9.2.2 Эрүүл мэндийн мэдээллийн системийн хэрэглэгч бүр үсэг болон тооноос бүрдсэн 10-аас доошгүй тэмдэгт бүхий нууц үг ашиглана. Дараах хэлбэртэй нууц үгийг хэрэглэхийг хориглоно. Үүнд:

- Толь бичигт байдаг үг
- Өөрийн болон төрөл төрөгсдийн нэр
- Регистрийн дугаар
- Утасны дугаар
- Компьютерийн гар дээрх тэмдэгтүүдийг дарааллын дагуу оруулах зэрэг болно.

9.2.3 Байгууллага тус бүр өөрийн өгөгдлийн санг тусгай зориулалтын төхөөрөмжүүд /Tape Drive, Storage Device, Backup server/-ийг ашиглан өдөр бүр нөөцөлж авах ба газарзүйн 3-аас доошгүй өөр байршилд хадгална.

9.3 Тандах арга хэмжээ

9.3.1 Мэдээллийн системийн нууцлал, аюулгүй байдалд тухайн байгууллагын дарга, захирал удирдан зохион байгуулж, тандалт хийнэ.

9.4 Залруулах арга хэмжээ

9.4.1 Тандалтаар илэрсэн сул талуудыг арилгана.

9.4.2 Халдлагад өртсөн тохиолдолд шалтгааныг тогтоон баримтжуулна.

9.4.3 Алдагдсан болон гэмтсэн мэдээллийг нөөц хувилбараас сэргээнэ.

10. Эрүүл мэндийн цахим мэдээллийн нууцлалын талаархи оролцогч талуудын эрх үүрэг

10.1 ЭМЯ-ны чиг үүрэг

10.1.1 Цахим мэдээллийн нууцлал, аюулгүй байдлыг хангах бодлогыг тодорхойлж, хэрэгжилтийг зохицуулах;

10.1.2 Цахим мэдээллийн нууцлал, аюулгүй байдлын эрсдлийн үнэлгээг хийх үйл ажиллагааг зохион байгуулах;

10.1.3 Төрийн болон төрийн бус байгууллага, аж ахуйн нэгж, иргэнээс цахим мэдээллийн нууцлал, аюулгүй байдлыг хангах талаар явуулж буй үйл ажиллагаа, гаргасан санал, санаачлагыг дэмжин туслах, тэдний оролцоог нэмэгдүүлэх, арга зүйн удирдлагаар хангах;

10.2 Эрүүл мэндийн байгууллагын дарга нарын чиг үүрэг:

10.2.1 Цахим мэдээллийн нууцлал, аюулгүй байдлыг хангах арга хэмжээг байгууллагын түвшинд зохион байгуулах, хяналт тавих;

10.2.2 Журмыг хэрэгжүүлэхэд шаардагдах хөрөнгийн эх үүсвэрийг бий болгох;

10.2.3 Байгууллагын түвшинд цахим мэдээллийн нууцлал, аюулгүй байдлын эрсдлийн үнэлгээг хийх үйл ажиллагааг зохион байгуулах;

10.2.4 Байгууллагын мэдээллийн нууцлал, хамгааллыг олон улсын ISO 17779, 27779 стандартын түвшинд хүргэхийг зорьж ажиллах.

11. Хариуцлага

11.1 Энэхүү журмыг зөрчсөн албан тушаалтанд холбогдох хууль, тогтоомжид заасан хариуцлага хүлээлгэнэ.