Análise dos dados – P6. Dados e manipulação de dados

1. Dados das entrevistas

Variável dependente - Participante

P6.V1.1

P6.V1.1 – P1ULSNA#01	Não me parece, acho que não estão cientes. Ainda continua a existir muito a tradição de trabalhar com aquilo que é meu, e não de haver esta partilha. Ontem comentava com uma profissional de saúde da necessidade de partilha de informação. Um dos serviços da PDS que mais vantagens trás é sem dúvida o serviço de urgência. Quando conseguimos colocar o sistema de informação que utilizamos na urgência a consultar a PDS, foi uma grande vitória, tendo sido a recetividade dos profissionais de saúde bastante positiva. Contudo através de observação no local verifico que os profissionais de saúde não utilizam a PDS. Ou seja continua a cultura de utilizar aquilo que é meu! De certa forma as pessoas depois de obterem os dados, de certa forma têm a ideia que podem fazer tudo o que querem com esses dados.
P6.V1.1 – P2ULSNA#02	Penso que na sua forma mais abrangente não existe uma clareza muito bem definida em relação a isto. Existe uma clareza muito grande na área da segurança, uma vez que se sabe quais os meios técnicos necessários a um sistema seguro, muito associada ao domínio específico dos técnicos de informática, enquanto responsáveis de sistemas de informação. Mas olhar para os dados em si como um universo paralelo à segurança física, acho que não existe essa noção. Em relação a este conceito que é transversal a todas as instituições, e que se tem vindo a arrastar no tempo, penso como técnico e também como utilizador de tecnologias, as pessoas acham que desde que o meio físico esteja protegido está tudo bem, os dados foram sempre descartados para segundo plano. Dá-se muita atenção à violação e ataque ao meio físico e não aos dados. Ninguém tem os seus dados encriptados no seu computador ou disco portátil.
P6.V1.1 – P2ULSNA#03	Estão, mas não suficientemente conscientes sobre esta questão. Há sempre situações que têm que ser colocados à comissão nacional de proteção de dados. Para a troca de dados com outras organizações existe uma consciência sobre os limites e regras de utilização.
P6.V1.1 – P1USF#01	Estão cientes até certo ponto. Não estão bem cientes daquilo que pode acontecer caso as coisas corram mal. Não pensam muito nestas questões. Veja-se o caso em que as pessoas partilham dados através de meios que não são institucionais.
P6.V1.1 – P2USF#02	Eu acho que há algumas organizações que até estão. É um assunto, que se não é atual, é um assunto muito falado. Começa a ser um aspeto muito cultural. Depende muito da preparação organizacional para estas matérias. No nosso caso, na saúde, e com a validação da CNPD, todos nós temos preocupações com os dados. Todos temos obrigações para cumprir.
P6.V1.1 – P3USF#03	Acho que neste domínio falta formação. No caso da PDS o manual apenas nos ajuda a utilizar a plataforma em termos informáticos. Não é propriamente um guia de privacidade, de como utilizar os dados. Deveria haver uma maior informação sobre as tarefas que podemos fazer em relação aos pessoais, o que não podemos fazer. Existe uma necessidade em saber os cuidados a ter com dados sensíveis. Nunca nos foi explicada esta situação. À partida, e com base na nossa formação sabemos mais ou menos os nossos limites, mas podemos cometer erros. Era importante haver uma maior sensibilização, mesmo cultura.
P6.V1.1 – P3USF#04	Eu acho que todos nós temos a preocupação que eu lhe falei, a preocupação relacionada com o nosso sigilo. As limitações podem não estar bem presentes, estão presentes de uma forma relativamente empírica. Aprofundar o conhecimento sobre esta temática seria importante. Os limites que nós conhecemos poderão não ser os ideais. Penso que é uma questão em que as pessoas não estão muito sensibilizadas, em relação ao que pode acontecer depois dos dados estarem registados no sistema. Existe aquilo que nos foi incutido, é uma coisa ética, de como profissionais de saúde guardar sigilo em relação aos dados. Agora essa parte técnica, do dia-a-dia de um

	sistema de informação é complicada.
P6.V1.1 – P3USF#06	Não, há muita falta de informação e de conhecimento nesta matéria. Ainda na semana passada estive numa reunião de embaixadores da PDS, e uma colega dizia "que não conseguia ver nada do hospital X", por falta de conhecimento em relação ao acesso à informação. Ao nível da USF, as pessoas têm algum conhecimento sobre o que podem fazer com os dados, mas não sei se será suficiente. Têm algum conhecimento sobre os limites. Todos os anos utilizamos em auditoria internas, dados clínicos, e as pessoas têm a noção dos cuidados a ter com os dados, temos sempre o cuidado de salvaguardar a identificação das pessoas. Como um todo as organizações, neste domínio, começam a estar melhor preparadas, também porque a formação académica que vamos tendo contribui um pouco. A cultura diferente associada às USF, assim como a exigência, facilita a passagem de informação sobre proteção de dados (…) Esta maior atenção na importância dos dados, desperta um maior interesse pela sua segurança.
P6.V1.1 – P1INEM#01	As organizações estão sensíveis, agora se isso acontece como o desejaríamos, se calhar não. Porque, por exemplo o nosso caso, em que cada vez mais utilizamos dispositivos móveis, e alguns com dados sensíveis, em que é necessário uma noção clara do que se pode fazer. Existe muito trabalho a fazer nesta matéria.
P6.V1.1 – P2INEM#03	Não me parece que estejam hoje em dia. Mesmo que algumas, embora tenham preocupações e possam demonstrar essas preocupações, creio que não estão totalmente a par de tudo. Nós próprios não estamos e temos que pedir pareceres à CNPD para saber o que é que eles têm a dizer sobre a utilização de um determinado programa ou de um determinado produto. Ou seja não existe ainda uma grande divulgação, uma grande cultura de uma forma geral neste domínio.
P6.V1.1 – P2INEM#04	Acho que a maior parte não.
P6.V1.1 – P2INEM#09	Eu acho que não. As organizações de um modo geral, pensando neste caso apenas [na área] da saúde, cada organização, ou cada grupo de organizações, com realidades de utilização de dados distintas […], têm uma coisa em comum – a intensidade na utilização de dados. Como as realidades [de utilização de dados] são diferentes, as pessoas vão reagindo com base naquilo que lhes vai acontecendo, e não há uma planificação prévia, ou um estudo prévio que diga em relação aos dados, quais os limites. […]
P6.V1.1 – P2INEM#10	Penso que não. É uma preocupação, e hoje em dia quem não falar em proteção ou privacidade de dados não está na moda! Mas as organizações não estão cientes das reais necessidades e dos reais problemas que têm. Assim como dos limites que têm, quando têm dados. No nosso caso [INEM] existe uma grande preocupação em relação à confidencialidade dos dados que temos em nossa posse. Mas sei que existem muitas organizações em que qualquer pessoa utiliza os dados. Não existe a preocupação com a proteção dos dados.
P6.V1.1 – P3INEM#05	Existe uma consciência destes limites. Na minha opinião o cruzamento de dados é extremamente importante, pois fornece ao profissional um conhecimento mais completo, completamente diferente. Antigamente não havia nada disto. Temos consciência que é necessário uma atenção especial nos dados.
P6.V1.1 – P3INEM#06	Não. As pessoas não conhecem os limites. Eu próprio tenho alguma dificuldade, em algumas situações, de perceber até onde se pode ir. E no meu caso lido com poucos dados em comparação com uma urgência onde são utilizados um conjunto maior de dados. O grande dilema é – temos certa informação que sabemos que se for partilhada pode trazer benefícios, em outras situações pode comprometer. É necessário mais informação sobre direitos e deveres no que toca à utilização de dados. A chave disto tudo é a formação e a educação das pessoas, dos profissionais de saúde. A tendência é cada vez haver mais haver partilha de dados, com muitos benefícios, nomeadamente através da PDS, mas vai ser necessário ter-se muito cuidado. E estes cuidados não nos podemos cingir só à proteção de dados e às medidas de segurança. Temos que começar na base que são os profissionais que lidam com os doentes e que necessitam e lidam com esta informação. Esta é a base. A única forma de controlar esta base é através da formação e educação dos profissionais. Mais conhecimento.
P6.V1.1 – P3INEM#07	Não. Não é a sua postura. À partida as organizações só se preocupam em recolher informação, e só depois se preocupam a em a proteger. Isto está virado ao contrário. Deveria pensar-se antes em como manter a informação sigilosa. Deveria haver uma maior atenção em relação aos dados que se recolhem, como são utilizados.

P6.V1.1 – P1HFF#01	Acho que não. Por isso é que existe a comissão de informação clinica, em que situações de envio de informação para o exterior são analisados.
P6.V1.1 – P2HFF#02	Não, porque toda a gente dentro do hospital pensa que está debaixo de um "guarda-chuva" de privacidade, pelo facto de trabalhar para o hospital. O facto de nós sermos colaboradores do hospital faz com que nós estejamos "protegidos". Mas não estamos num extremo, em que pelo facto de estarmos aqui, podemos fazer tudo e mais alguma coisa com os dados. Sabemos que existem alguns limites. Agora o conhecimento destes limites é que não é muito claro. Em relação à partilha de dados com outras organizações são levantadas sempre questões. Porquê estes dados? Porque estamos a partilhar estes dados? Qual o objetivo da partilha destes dados? Deveria haver um maior conhecimento partilhado sobre os limites relacionados com a partilha de dados entre organizações, nomeadamente através da PDS. Nos próximos desenvolvimentos da PDS deveria acautelar-se melhor estas questões. Nomeadamente com o acesso dos privados à PDS. O facto de a PDS depender da RIS tira algumas preocupações, mas, se todos cumprirem com os requisitos de segurança da RIS. Existem muitos pontos de falha.
P6.V1.1 – P2HFF#03	Não sei se estão cientes. Mas se estão cientes não fazem nada. O mais certo é terem outro grau de preocupação. Por exemplo se um hospital está preocupado em que as pessoas registem não quer por barreiras. E portanto tudo o que toca com privacidade nesta altura é indutor de barreira. Quando se quer que os clínicos adiram à PDS, falarem em mais esforço por causa da privacidade pode ser indutor de barreiras. Neste momento a preocupação é outra. Muitas vezes estas questões funcionam pela ocorrência. Eu não tenho dúvidas que num futuro próximo, algumas destas questões vão-se colocar de forma muito premente por razões legais. Ou seja, porque vai acontecer alguma coisa de errado, vai alguém usurpar a identidade de um médico, o que vai induzir em medidas. Eu não tenho dúvidas que as organizações não estão a ser proactivas, a não ser que haja uma orientação de cima para baixo com um modelo. Só por fatores exógenos, e no sector da saúde a mudança tem acontecido exclusivamente por fatores exógenos. De uma forma endógena é raro as coisas acontecerem.
P6.V1.1 – P3HFF#04	Não estão cientes. Podem ter subjacente no seu dia-a-dia esta noção, mas porque efetivamente, não existe, tanto quanto eu sei, nas organizações, nenhum grupo ou comissão que tenha como missão dentro da organização ser o orquestrador de tudo isto. Não temos de facto a consolidação destes conceitos em si. Na colaboração com outras organizações a noção do que podemos ou não partilhar não existe. É necessário um maior conhecimento coletivo destas questões, e sobretudo algumas orientações. Até porque os dados resultantes dos registos da informação em saúde, da nossa população, dentro da organização têm um determinado peso, valor e preocupação, mas num contexto de partilha externa terão outros.
P6.V1.1 – P1SPMS#02	A maior parte das instituições tem algumas noções mas não uma visão clara de todas estas questões. Em relação à partilha de dados, nomeadamente através da PDS, os profissionais necessitam de ser melhor esclarecidos. No entanto os dados são disponibilizados aos profissionais e sabemos que as pessoas a consultam, mas deveria haver um regulamento sobre as restrições na utilização dos dados – os dados podem ser utilizados, não podem ser copiados, nem reproduzidos num outro suporte. É necessário explicar de uma forma clara quais são os limites. É também uma questão de ética profissional. O acesso ao portal do profissional só está disponível dentro da RIS. Os profissionais acedem no contexto da aplicação. Garantimos a segurança e controlo dentro da RIS. Está a ser estudada a possibilidade de um portal na Internet, mas com reforço de segurança. Não vamos divulgar dados das instituições ao setor privado. Estamos a falar de um projeto em específico, em que se acede apenas a uma funcionalidade.
P6.V1.1 – P2SPMS#03	Tipicamente quando um produto chega a uma instituição, está dá início à sua utilização. Não está consciente sobre as limitações que tem em relação à sua utilização. Nos últimos anos tem-se vindo a fazer um esforço no sentido de consciencializar, que ainda que o produto seja desenvolvido pelo ministério da saúde, que o mesmo tem que ser notificado e repostado junto da CNPD. Tem sido feito um grande esforço para que isto seja uma realidade.

	Mas acredito que isto é visto como uma limitação ou um entrave e não como um caminho a seguir. Existem ainda hoje casos em que as pessoas têm a noção que podem fazer tudo com os dados.
P6.V1.1 – P2SPMS#04	Devem ser poucas as organizações que estão cientes. Existe muito trabalho a fazer. Neste domínio deveria também entrar a questão da semântica, de modo a todos falarmos o mesmo, sabermos do que estamos a falar. Está muito relacionado com a taxonomia que e falamos. Como é que a gente consegue dizer que estes dados são cíticos e só devem ser vistos pelos psiquiatras, se não tiver uma classificação?
P6.V1.1 – P1HES#01	Em relação à recolha e à utilização de dados acho que as organizações não estão cientes dos limites. Em relação ao que podem recolher têm imensas dúvidas. Alguns grupos profissionais têm algumas noções destes limites. Outros grupos nem tanto. Só conseguimos melhorar este cenário através de sensibilização que falamos, que não existe ainda. Quando as pessoas chegam, mesmo com formação é insuficiente. Mesmo em relação à partilha dos dados, acho que as pessoas não estão cientes do risco. Cada um de nós sabe, mas por bom senso, e não porque alguém nos disse ou informou. Não existe nenhum "manual" ou regras definidas. O que pode ou não ser partilhado é assim decidido com base no bom senso. Alguns profissionais de saúde ficam furiosos quando são alertados para determinado risco, porque não percebem que não faz sentido nenhum de acordo com a legislação. Não conhecem os princípios de proteção de dados. Mesmo aos sistemas de informação são pedidos dados que colocam em causa os princípios de proteção e dados, e que nós muitas vezes recusamos responder. Muitas vezes nem tem a ver com a cedência de dados mas com a filtragem de dados dentro de uma base de dados. Que não se pode fazer.
P6.V1.1 – P2HES#02	Eu acho que ainda não estão bem cientes. Ainda há muitas limitações na parte decisora, de quem está à frente das instituições. Tendo algumas limitações, não recorrem a quem ainda possa ter algum conhecimento, no sentido de ajudar quando surgem dúvidas. Tentar perceber o que podemos ou não desenvolver. Que riscos é que podemos ter. Normalmente alguns dos decisores não têm esse conhecimento, não quando há dúvidas não procuram soluções. Normalmente quando surgem dúvidas recorremos à CNPD. Internamente, não temos um especialista em proteção de dados. Em algumas questões valemos também do gabinete jurídico. Em privacidade dos dados o próprio jurista tem limitações. Para os sistemas de informação as leis são mais específicas. Dependem de um conhecimento específico em sistemas de informação.
P6.V1.1 – P2HES#03	Penso que não estão o suficiente. O medo de acontecer alguma coisa [das consequências] é que ajuda a evitar certos problemas. Nunca partilhamos dados para fora, apenas por sabermos que podem acontecer problemas. Neste momento não existe uma noção clara do que podemos partilhar.
P6.V1.1 – P3HES#05	Acho que as pessoas têm consciência de que é limitado o que estão a recolher. Têm ideia que existe uma fronteira, pouco clara. As pessoas não refletem muito sobre isto. É importante e interessante mais conhecimento sobre isto, nomeadamente com formação obrigatória. Todos os profissionais deviam refletir sobre este impacto das novas tecnologias e na forma como devem lidar com a confidencialidade dos dados, a segurança dos dados, os dados, o que registar, como registar. Nos últimos dez anos, eu tenho doentes que têm 140 episódios. Isto é ingerível. Ninguém consulta esta informação. Portanto, para que serve esta informação? É uma quantidade avassaladora de informação. Precisamos de periodicamente fazer uma revisão dos dados dos doentes com mais episódios, e havendo uma pessoa gestora daquele doente, ter a responsabilidade de fazer uma revisão dos dados – passar para um histórico o que não é importante. Para mim isto faz sentido. Algumas plataformas de registo são tão complexas que as pessoas para não andarem de "caixinha em caixinha", arranjam uma "caixinha" onde registam tudo. O que pode fazer com que outros posteriormente não consigam ver nada. Deveria ser claro, onde registar, em que sitio, em que local, o quê, e o que posso partilhar ou não. Autorizo ou não a partilha. O que interessa mais partilhar é o diagnostico, e se calhar é aquele que a pessoa não quer partilhar. São dados mais confidenciais. Quem tem competência para colocar codificação clinica são os codificadores clínicos. O que a PDS e a nota de alta querem é que se

	utilize codificação clinica, e isto não é possível. A partir daqui podem surgir muitos dados errados.

P6.V1.2

P6.V1.2 – P1ULSNA#01	A destruição é fundamental. Era fundamental quando se utilizada arquivos em suporte papel, por forma a garantir a privacidade da informação. No meio digital as questões da privacidade surgem muito na fase de criação e utilização de dados e começam a surgir maiores preocupações na transferência de dados. O armazenamento e arquivo hoje estão mais ligados a questões de segurança.
P6.V1.2 – P2ULSNA#02	Fazem todas parte do mesmo processo. Basicamente os dados são gerados, e até alguém os destruir ou apagar, eles vão existir, seja em meio físico, em papel ou em digital. Existem regras comuns para a duração do arquivo em papel, sendo efetivamente alguns dados destruídos passados 10 ou 20 anos. A informática não tem responsabilidade sobre a destruição de dados, depende das indicações da área administrativa responsável ou do conselho de administração. A nossa concentração é a criação e utilização dos dados, nomeadamente na unificação de processo de pessoas mal identificadas, que geraram processos paralelos. Existem episódios que não obrigam a criação do seu processo físico (como é o caso do atendimento em urgência de cidadãos estrangeiros). Para os restantes é automaticamente criado um número de identificação de processos e os serviços arquivo criam uma nova estrutura em papel com todos os documentos inerentes. Este processo em papel, têm regras para a sua destruição. Nos dados digitais não temos esta preocupação.
P6.V1.2 – P2ULSNA#03	A transferência principalmente. A criação e utilização não é muito uma preocupação porque, e neste caso em relação aos dados dos utentes, para as aplicações que nos chegam, não concebidas por nós, normalmente limitamo-nos a preencher dados que as aplicações nos pedem. Agora quando existe uma transferência, nós temos que perceber o que é que vai ser transferido. Por exemplo na radiologia, em que temos alguns protocolos com outras organizações, o exame nunca vai acompanhado com dados de identificação do utente. A pessoa que recebeu os dados, faz o relatório do exame, e quando este é devolvido, é junto aos dados iniciais. Existe de certa forma uma preocupação com a privacidade. No arquivo e destruição não temos muito essa sensibilidade. Temos alguma preocupação com as imagens, colocadas num local, que só é utilizado em casos específicos.
P6.V1.2 – P1USF#01	A utilização é uma das fases mais importantes. Os dados do utente nunca são destruídos. Os dados permanecem nos sistemas, nas bases de dados, mas deixam de estar acessíveis, existem alguns condicionamentos no acesso a estes dados. Os dados não são anonimizados. A transferência de dados, os sistemas começarem a utilizar os dados uns dos outros, que é aquilo que a PDS faz, preocupa-me, essencialmente porque muitas vezes as pessoas não tendo noção daquilo que estão a utilizar, quer dizer as pessoas sabem o que estão a utilizar, só que em situações de muito trabalho, a proteção dos dados deixa de ser prioritária, e podem existir situações de exposição dos dados. Ao nível da infraestrutura, servidores, existem mecanismos suficientes para garantir a segurança. Tudo depende das pessoas.
P6.V1.2 – P2USF#02	Existem várias fases, dependendo do tipo de dados e dependo inclusive das normas da CNPD para vários tipos de dados, vários tipos de informação. Há fases que são sempre preocupantes. Por exemplo a fase da destruição de dados tem que ser garantida, segura e validada. É uma fase crítica e preocupante. Neste aspeto a CNPD em algumas bases de dados é muito rigorosa, especificando o espaço temporal de utilização dos dados – cabe aos responsáveis pelos sistemas de informação controlar estas situações e averiguar se estas obrigações estão a ser cumpridas. Claro que o armazenamento de dados é muito importante, em que é necessário assegurar que os dados que temos estão seguros e devidamente utilizados. Os dados em produção têm que ter garantias de utilização correta.
P6.V1.2 – P3USF#03	Não vejo uma fase que seja mais preocupante (...). É a cultura da privacidade que tem que cobrir estas fases todas. Para os profissionais

	a privacidade em algumas destas fases como a utilização e transferência é transparente. Não questionam o funcionamento da privacidade, confiam á partida nos sistemas.
P6.V1.2 – P3USF#04	Acho que acabam por ser todas muito importantes. Se a preocupação em relação à privacidade pode ser comprometida em qualquer uma dessas etapas, não é muito inteligente protegermos uma ou outra etapa e comprometer outras. Qual é a vantagem de protegermos muito apenas uma etapa? (…)
P6.V1.2 – P3USF#06	Eu acho que todas as fases devem contemplar medidas. Preocupamo-nos, hoje em dia, muito com a transferência, mas todas as outras fases são preocupantes.
P6.V1.2 – P1INEM#01	Todas as fases são preocupantes, mas a destruição de dados pode ser uma das mais preocupantes. Na maioria das vezes não damos a devida importância à destruição. Já houve provas disso, quer na área da saúde como fora da saúde, que querendo ser malicioso existe muita informação disponível. A criação e utilização dos dados as pessoas conseguem algum controlo. A partilha de dados começa a preocupar as pessoas.
P6.V1.2 – P2INEM#03	O facto de termos os dados armazenados quase indefinidamente, há que pensar na mesma em todas as fases. Os dados não se alteram quanto à sua confidencialidade, tenham eles o tempo que tiver. O manter os dados quase eternamente, é algo que eu questiono – deveria pensar-se seriamente na destruição de dados. Apesar de os dados serem necessários para estudos, para análises. Mas em determinado momento os dados deixam de ser uteis, qual é a vantagem de manter estes dados? Nós por norma não eliminamos dados apesar de a norma nos indicar 5 anos de vida para estes dados. Apesar de mudarmos para um novo sistema em 2007, tudo o que são dados do sistema antigo até 2007 continuam a estar disponíveis numa base de dados […].
P6.V1.2 – P2INEM#04	Penso que todas as fases têm que ser pensadas como um todo, são todas muito importantes. Claro que os dados que estão em utilização são os mais sensíveis. Do ponto de vista técnico é o mais difícil. São mais as circunstâncias em que pode haver violação de dados. Quanto ao ciclo, eu não penso muito na destruição da informação. Naquilo a que eu me habituei a informação não deverá nunca ser destruída. A transferência de dados será sempre uma preocupação e têm vindo a aumentar.
P6.V1.2 – P2INEM#09	Este ciclo depende muito do que a lei nos diz. Por questões clinicas, judiciais, é necessário garantir a disponibilidade destes dados durante alguns anos. Sim todas estas fases justificam medidas de proteção para os casos em que se lida com dados identificáveis. Quando não se consegue associar dados a pessoas, o risco não existe. Ou seja, isto será tão mais importante quanto mais houver ligação de dados a pessoas.
P6.V1.2 – P2INEM#10	As fases iniciais, as de registo e utilização, são as mais preocupantes, mais criticas, mais sérias, em que os dados estão disponíveis à generalidade dos utilizadores. Tem que se pensar em políticas de privacidade para estas fases. Hoje está tudo em formato digital. Quando se chega a fase de armazenamento, os dados só já estão disponíveis a um grupo restrito de pessoas, que normalmente são gestores de sistemas, que não vão consultar a informação, nem querem saber o que lá está, em que consta. Os dados nesta fase estão bastante protegidos. Deixam de estar disponíveis à generalidade dos utilizadores. Quanto à destruição de dados, é muito difícil deitar informação "fora". Agora deve ser cumprido o prazo de vida dos dados. É verdade que a maioria dos dados deixam de ter interesse, devem ser destruídos. Outros podem ter interesse daqui a vinte anos, e devem ser protegidos, retirando informação de identificação. Seria uma política eficaz de privacidade.
P6.V1.2 – P3INEM#05	Penso que sim, algumas fases requerem mais atenção que outras. O arquivo por exemplo. Numa fase inicial quando entrei em funções, o papel arquivado era um problema e ainda o é – é necessário segurança. Recebemos uma auditoria externa em que um dos parâmetros *standards* exigidos era precisamente o arquivo, espaço isolado de acesso restrito. Em relação à transferência de dados entre

	instituições existe por parte das pessoas uma confiança inicial, que resulta do facto de lhes ser explicado que existe uma garantia e uma importância no que está a acontecer. No dia-a-dia comprova-se isso, quando as pessoas percebem que não há fugas, e se existirem - se não houver uma fuga, uma fissura na fronteira (das organizações) não havia noticias – sabem que pode haver consequências.
P6.V1.2 – P3INEM#06	Todas são preocupantes. Em algumas tem que se ter uma particular atenção. Na criação deve ser questionado se posso ou não recolher estes dados. Na utilização tem de se perceber para que se quer os dados e que dados é que se vão ser usados. Este é um aspeto fundamental, uma vez que eu só devo ter acesso aos dados que são importantes para as minhas tarefas profissionais e para bem do utente. Na mesma forma tudo o que transmito ou partilho a outro tem que ser nesta perspetiva. Tudo o que for a mais não interessa. A transferência de dados é um processo que cada vez vai ter que acontecer mais. A informação clinica (…) vai cada vez ser mais partilhada, inclusive com instituições fora da área da saúde (GNR, etc.) o que obriga a que se tenha cuidados na transferência. Há dados que são relevantes e há dados que não o são. Mais ou menos sensíveis. A informação que nós recolhemos, agrupada em vários grupos, como é o caso dos antessentes pessoais (doenças infectocontagiosas por exemplo), que é importante para os profissionais de saúde, que está no verbete, na informação clinica recolhida, mas que para quem vai investigar aquele acidente, os antecedentes pessoais não são relevantes. Ou seja diz respeito também à utilização. Para que é que estes dados vão ser usados? O armazenamento e arquivo são importantíssimos, mais que a fase de destruição. É importante que estejam bem armazenados, bem arquivados. Agora há dados que têm que obrigatoriamente ter um limite de utilização. E ai a forma como são destruídos é preponderante. Mas com base na realidade que eu conheço o armazenamento e o arquivo são mais importantes. Estas duas fases bem solidificadas, com barreiras bem definidas, bem organizados, no fundo é como se a destruição seja apenas uma mais-valia.
P6.V1.2 – P3INEM#07	De uma forma genérica todas estas fases deveriam ter uma atenção específica. Mas a armazenagem e destruição deveriam ter uma atenção especial. Mesmo em digital, depende do fim para que guardamos informação eternamente. Se for tida como necessária para a realização de estudos científicos estou de acordo com a sua continuidade de utilização, senão tem que ser eliminada. Claro que são necessárias medidas que protejam sempre a identidade dos doentes.
P6.V1.2 – P1HFF#01	Normalmente não nos preocupamos com a destruição. Normalmente não existem normativos, sensibilidade, porque o pensamento que existe é que "é mais importante que um dado exista do que não exista". Só o facto de que a informação ser importante para gerir, para histórico, dificilmente vai ser destruído histórico, nomeadamente dados relacionados com os doentes. Muitos dados são importantes no suporte à investigação. Agora são necessárias medidas específicas para a utilização destes dados.
P6.V1.2 – P2HFF#02	Todas elas deveriam ter medidas específicas. Há umas que preocupam mais, nomeadamente o armazenamento, transferência e o arquivo. Na criação e utilização nem tanto, apresar de ser previstas algumas medidas, nomeadamente na análise de que dados necessitamos, se são supérfluos. A saúde está em primeiro. Podem existir casos onde não faz sentido a recolha de determinados dados, mas com a prática clinica algo subjetiva, em que não existe normas abrangentes, isto pode acontecer. Quanto à destruição de dados, nós não destruímos dados, mesmo que administrativos. O hospital para além de ser uma unidade de cuidados de saúde também é uma unidade de investigação e desenvolvimento, dai a não destruição de dados. Deveria isso sim haver algumas regras de proteção destes dados. É necessário uma preocupação a este nível.
P6.V1.2 – P2HFF#03	É um tema muito interessante, pois neste momento nós estamos a registar dados e não nos estamos a preocupar com a qualidade desses dados durante um determinado tempo. Ou seja, durante quanto tempo fazem sentido esses dados. E nós vemos que uma taxonomia, ou uma definição – que tipo de dados, devem durar que tempo – faz todo o sentido. Veja-se a imagiologia, se uma mamografia faz sentido vários anos, um raio x deixa de fazer sentido passados um ano ou dois. No entanto estar a guardar informação que ocupa espaço, cada vez mais espaço, e que não tem interesse clinico só vai complicar a vida ai clinico no momento da decisão,

	porque tem mais informação onde tem que procurar. Nós também não temos nenhuma orientação sobre como destruir, passar para um 2º plano, digamos assim, em *offline*, acessível mas num contexto mais complexo. Muito do trabalho que nós temos feito agora consiste em dar a informação certa num contexto. Se eu estou numa urgência o que quero ver a informação necessária [...]. Muita informação com o tempo perde contudo interesse clinico. Esta informação pode permanecer no sistema, uma vez que pode vir a fazer falta, mas deve passar para uma *data warehouse* e estão lá, são acessíveis na mesma, mas não estão é naquele *front-end* quando o médico tem que tomar uma decisão. Tem a ver com a qualidade da estrutura de dados. Se os dados forem bem estruturados é fácil eu estipular regras e poder padronizar. Se eu tiver uma informação apenas digitalizada, tenho um problema maior. Temos alguma informação digitalizada – a que vem do INEM, ofícios, cartas, credenciais, consentimentos. Esta informação tem um valor muito parco no tempo. Interessa naquele episódio, só serve para qualquer coisa naquele contexto. Alguma pode ter interesse futuro, até legal. E muitas vezes as questões de interoperabilidade são um problema, porque os dados estão espartilhados por vários sistemas, e eu tenho uma dificuldade em juntar esta informação para responder a uma determinada solicitação. Hoje se um paciente quiser o seu processo clinico nós estamos habilitados a dar, se calhar, uma informação muito interessante, mas não lhe conseguimos dar todos os dados. Porque o esforço que temos feito é da transversalidade e portanto ter informação que é o tronco comum. Se um utente solicitar o seu processo clinico nós damos-lhe um subconjunto do seu processo clinico.
P6.V1.2 – P3HFF#04	Não é bem a minha área, mas tínhamos que ter em suporte papel, o arquivo dos registos durante vários anos porque poderia ser necessário rê-entrevir sobre esse utente. A janela temporal era aquela que se considerou adequada para várias áreas, e sempre com o pressuposto que aquilo poderia ser importante para uma auditoria retrospetiva sobre ação ou conjunto de ações num individuo. Hoje em dia esta janela temporal tanto quando eu sei é infinita. Uma especificação muito concreta – em situações de dados relativos a doenças de heredo-familiares, não se pode anonimizar os dados identificadores. Havendo regras de privacidade também para a situação do arquivo e eliminação, têm que ser criadas exceções para situações como a que lhe apresentei.
P6.V1.2 – P1SPMS#02	Todas estas fases são preocupantes. Não devo estar a destruir informação que possa vir a ser útil. Em termos de privacidade dos dados todas estas fases do ciclo de vida da informação importantes. Tenho alguma dificuldade em ver a necessidade de medidas específicas em cada uma das fases e quais as medidas de privacidade a aplicar, mas acredito que tenha que se aplicar determinadas medidas em cada uma das fases e estudar essas medidas.
P6.V1.2 – P2SPMS#03	Eu diria que todas elas devem ser preocupantes em termos de privacidade. Tipicamente, não conheço nenhum projeto na saúde que se preocupe com o arquivo, em termos de histórico da informação. Isto é um ciclo de vida da informação, de como ela é criada, é gerida, é mantida, é corrigida, etc., ao longo do tempo de vida. Ainda bem que existem entidades como a CNPD, que é a entidade que vai obrigando a que as entidades pensem mais um pouco sobre o assunto. Pelo menos que façam o registo daquilo que estão a fazer em matéria de utilização de dados. Ao fazerem questões, obrigam as pessoas a serem mais criativa, a arranjarem soluções. De qualquer das formas deveria ser obrigatório a notificação e quais alterações que acontecem no espaço temporal. Não existe sequer o conceito de destruição de dados. As nossas bases de dados têm "*terabytes*" de 20 anos, de mais fácil acesso. A informação em papel representava um risco menor em termos de privacidade do que um dado eletrónico. A privacidade dos dados só se coloca com esta facilidade de acesso dos meios tecnológicos.
P6.V1.2 – P2SPMS#04	Em termos da proteção da privacidade, temos um problema cada vez mais grave dado o aumento do volume de informação, em que acedemos a milhões de registos. Andamos a tentar fazer com que alguns dados passem a dados históricos. A questão é, o que é que vamos passar? O que é que tem que estar disponível ao médico para o suporte à sua prática do dia-a-dia, e o que é que pode passar para

	histórico? Ainda ninguém sabe, ninguém ainda fez ou trabalhou esta área. E começa a ser crítico por já não temos capacidade de disponibilidade destes dados nas bases de dados. Deveríamos pensar no arquivo e mesmo na própria destruição e dados. Apesar de destruição mesmo nunca vai haver, pois os dados passam apenas para uma base de dados secundária. É necessário definir o tempo em que os dados ficam no sistema principal, e contemplar as situações em que temos que fornecer dados ao exterior, como pedidos vindos do tribunal sobre determinado processo clinico.
P6.V1.2 – P1HES#01	Nós não destruímos coisíssima nenhuma! Nos registos em papel ao fim de X tempo, os registos eram enviados para outro edifício dentro da cidade. E depois ao fim de alguns anos eram destruídos. De uma forma diferente são todas importantes. Todas elas são importantes. Sendo que a utilização e a transferência são onde recaem as maiores preocupações. Uma má utilização é sem dúvida mais preocupante. Sobre o arquivo e destruição, os dados, mesmo no setor da saúde, não devem ficar eternamente nos sistemas. Mas nós temos. Nós não apagamos nada. Em termos de arquivo, por exemplo tudo o que tem a ver com imagem, ficheiros grandes, nós temos um arquivo de curta duração que tem 5 anos, e depois temos um arquivo de longa duração, em que todos os exames com mais de 5 anos passa para este arquivo. Sempre que a informação for vital e importante deve ser mantida nos sistemas. Temos que pensar em medidas específicas. Agora surge a questão – quem é que define estas medidas específicas? A velocidade de evolução dos sistemas de informação não foi acompanhada pela legislação em proteção de dados.
P6.V1.2 – P2HES#02	Em matérias de privacidade eu acho que as mais preocupantes têm a ver com a utilização, transferência e armazenamento. Quanto ao arquivo, e que eu tenha conhecimento, nós não fazemos destruição de dados. A parte da destruição poderá não fazer algum sentido, até porque grande parte da informação tem a ver com processos clínicos. Enquanto a pessoa for viva temos que ter o seu processo clinico. Mesmo depois da pessoa ter falecido é necessário a manutenção desta informação. Fundamental é a assim a utilização, o armazenamento e a transferência. Mesmo que os dados tenham que ser destruídos, têm que ser por um profissional habilitado para o caso, em procedimentos que garantam essa destruição. A proteção dos dados em arquivo deve permitir a identificação da pessoa, por forma a poder fazer uma reconstituição ou suportar um estudo sobre a família em causa.
P6.V1.2 – P2HES#03	Todas estas fases são preocupantes, em matéria de privacidade dos dados. Claro que os dados mais recentes são mais preocupantes. Dados em arquivo, com mais de 5 anos, também são preocupantes, mas não como os dados em utilização. São contudo fundamentais à história clinica do utente. Não temos medidas específicas para destruição de dados. Os dados ficam até se necessitar de espaço. Em termos de arquivo os dados são armazenados em *tapes*, protegidos apenas por medidas de segurança. Medidas de privacidade não são ainda implementadas.
P6.V1.2 – P3HES#05	A criação é o mais crítico. É o momento para o qual muitas pessoas ainda não perceberam que um registo de diagnóstico pode ser essencial para o utente daí a 5 ou 6 anos. Pode ser um co fator para uma outra gravidade. [...] É essencial que no registo o profissional se comprometa com aquilo que pensa. [...] Os dados da saúde não podem ser eliminados. Temos os sistemas subcarregados de informação. Anualmente estes registos deveriam ser transferidos do ativo para o inativo, tipo armazenamento.

P6.V2.1

P6.V2.1 – P1ULSNA#01	É, mas estamos a falar do sector da saúde, que acaba por lidar com as pessoas em situações sensíveis, e queiramos ou não, para um determinado assunto as pessoas não se preocupam com a sua privacidade. Querem apenas ter serviços de saúde. Como responsável do sistema de informação reconheço que todos os processos de recolha e de tratamento de dados não estão

	claramente documentados e conhecidos, sabe-se qual o objetivo da recolha dos dados, mas não se conhece as limitações da sua utilização.
P6.V2.1 – P2ULSNA#02	Claro, concordo a questão. Até podem existir campos que nem sequer são utilizados, ou mesmo mal utilizados. É vantajoso haver esta consciência para que os dados servem.
P6.V2.1 – P2ULSNA#03	Sem dúvida, era aquilo que eu dizia inicialmente – quando se concebe uma aplicação, temos que conhecer a sua realidade de aplicação, caso contrário podemos estar sujeitos a fugas. Penso que a maioria das pessoas não tem conhecimento sobre os objetivos da recolha dos dados e as limitações na sua utilização.
P6.V2.1 – P1USF#01	Os dados que são recolhidos servem essencialmente para prestar um melhor serviço ao utente. Agora é importante, acima das questões de segurança, as pessoas olharem para estas questões com outra atenção. Ainda não se pensa muito nisto mas é importante uma maior atenção. Tudo leva sempre à mesma questão. Quem são as pessoas e qual a utilização que fazer dos dados. Podem existir profissionais que podem deturpar a utilização de dados, e utilizar estes dados para outros fins.
P6.V2.1 – P2USF#02	Acho que trabalhar em equipa é muito bom. E se toda gente souber e a trabalhar para o mesmo fim, mesmo a níveis diferentes. Provavelmente um conhecimento massificado dos objetivos da utilização de dados facilitava a compreensão de medidas de proteção de dados.
P6.V2.1 – P3USF#03	Sim muito.
P6.V2.1 – P3USF#04	Claro que sim, facilita.
P6.V2.1 – P3USF#06	Claro que sim, é mais fácil perceber as medidas de proteção desses dados. Quando recolho dados junto do utente, eu tenho que explicar ao utente porque estou a recolher aqueles dados. A maioria dos profissionais de saúde tem um bom conhecimento sobre a razão da recolha de dados.
P6.V2.1 – P1INEM#01	Sim e perceber quais são os seus limites. Facilita-se depois o desenho daquilo que é a privacidade. Infelizmente, não é uma prática nossa, a documentação, justificação e enquadramento de cada processo. Ao sermos uma instituição de saúde com um objetivo muito específico entendemos que a lei geral não se aplica a nós. Este entendimento pode estar errado. Mas este é um assunto que nos preocupa, até para nos justificarmos perante instituições oficiais que nos controlam no sentido de demonstrar quais os princípios que não cumprimos. Sendo esta uma prática comum entre todas as organizações seria depois mais fácil desenvolver políticas de privacidade comuns e até para auditar e verificar se está ou não a ser cumprido. Até porque as instituições apresentam processos comuns de recolha de dados, o que pode ser uniformizado.
P6.V2.1 – P2INEM#03	Poderia ajudar, está muito dependente da cultura de cada um. Existem situações em que se recolhem dados em que a pessoa nem sequer tem a noção da legislação nem qualquer tipo de informação. Eu, de todo, forneço qualquer tipo de dados mais confidenciais se não tiver lá explicitamente dito para que servem os dados e como é que vão ser tratados. Não temos esta cultura incutida e a maior parte das pessoas não se inibe de fornecer os seus dados em qualquer formulário *online* que tenha de preencher.
P6.V2.1 – P2INEM#04	Sim. Normalmente os processos de recolha de dados não são documentados, pelo menos por nós. Limitamo-nos muitas vezes a desenhar os processos de acordo com as especificações que alguém determina. Agora penso que sim, deveria haver uma maior informação sobre o objetivo da recolha de dados. Seria para nós mais útil, no sentido de negociarmos certas especificações do sistema. Muitas vezes é-nos pedido para desenvolvermos uma ficha de recolha de dados, um determinado conjunto de campos, e dificilmente percebemos a importância, qual é o objetivo do processo. Já estive envolvido em projetos em que a não inclusão de uma pessoa especializada em proteção de dados, implicou que a informação foi lá colocada sem justificação, e que muitas vezes acabava por

	comprometer a eficiência da solução porque alguém achou que aquilo deveria lá estar.
P6.V2.1 – P2INEM#09	Sim, porque quando há uma recolha de dados deve haver uma preocupação com a utilização destes dados. Estes dados servem para quê? Em várias situações me interroguei sobre o porquê de eu estar a fornecer determinados dados. Aqui existe a preocupação de transmitir sempre o objetivo da recolha de determinados dados. As pessoas sabem para que vão servir os dados recolhidos. Se para as pessoas for suficientemente claro a utilização que se vai dar aos dados, facilita depois a introdução de políticas de privacidade. É muito importante saber qual é o objetivo. Qual a aplicação dos dados? Quais as consequências?
P6.V2.1 – P2INEM#10	Neste momento para o comum do cidadão esta não é uma preocupação. A maioria das pessoas fornece os dados sem questionar a sua utilização. Agora nas organizações [no meio da saúde], se se pretender implementar políticas rigorosas de privacidade é exigível às pessoas que conheçam o objetivo para que se está a recolher os dados. Facilita o que vem depois. No nosso caso [INEM] as pessoas sabem para que servem os dados. Mas é importante que as pessoas saibam qual é o objetivo da recolha de dados e das políticas a implementar. É importante ter em conta a cultura de privacidade existente.
P6.V2.1 – P3INEM#05	Com os profissionais com quem trabalho nunca identifiquei essa necessidade. Ou seja, naquilo que é o trabalho deles as pessoais queixam-se de terem mais dados do que os necessários. Numa fase inicial as pessoas registam dados e apresentam algumas dúvidas sobre o destino daqueles dados, mas depois percebem da sua importância, da sua vantagem. Com a experiência as políticas de privacidade são mais fáceis de compreender do que numa fase inicial. É importante nesta fase explicar às pessoas o que é necessário fazer e o porquê!
P6.V2.1 – P3INEM#06	Sim, as pessoas deveriam ter mais informação e estar mais informadas sobre os processos de recolha de dados. Tenho alguma dificuldade em desligar-me do meu papel, da prática clinica. Na prática clinica que nós temos, a maior parte de nós sabemos porque estamos a recolher os dados. Tem influência quer na minha atuação, quer na atuação do outro profissional a quem vou entregar o utente. Por isso neste sentido até temos esta informação, porque sabemos da pertinência da recolha, da maior parte das perguntas que fazemos e dos dados que recolhemos. Conseguimos perceber, porque sabemos, que mesmo que não influencie a minha atuação, sabemos que pode influenciar a atuação num hospital, ou outro local. Concordo que quanto mais se conhecer o objetivo das recolha de dados mais fácil é a compreensão da justificação das politicas de privacidade. Até porque as coisas estão interligadas. Se eu perceber o porquê da recolha de dados é mais fácil entender a razão da sua proteção.
P6.V2.1 – P3INEM#07	Os dados são recolhidos com um determinado fim. Em determinadas circunstâncias poderemos estar a recolher dados que não estão relacionados ou são em demasia. São dados recolhidos que estão ao lado da atuação que se está a ter. Não quer isto dizer que estes dados não possam ser uteis mais tarde. Qualquer processo de recolha de dados, bem esclarecido, facilita a proteção daqueles dados.
P6.V2.1 – P1HFF#01	Aquilo que é gestão da informação, pura e dura, é um facilitador para trabalhar as questões da privacidade. Posso agregar e definir políticas de utilização da informação. Sem dúvida que a organização da informação é sem dúvida um excelente ponto de partida. Até na atribuição de responsabilidades.
P6.V2.1 – P2HFF#02	Sim, perceber-se de uma forma clara e transparente, porquê estes dados, qual o objetivo da recolha destes dados. Por vezes recolhemos dados a mais e depois passado algum tempo verificamos que fazem falta a determinados estudos. Agora se houver um conhecimento geral sobre o objetivo da recolha de dados, facilita depois as medidas de privacidade. É prática comum dentro do hospital documentar todos os processos de recolha de dados, assim como a definição de um responsável setorial pelos processos de recolha de dados. Todo e qualquer processo de recolha de dados clínicos ou administrativos, são avaliados, e ai são documentados.

P6.V2.1 – P2HFF#03	Voltamos à informação, nós já tínhamos falado desta questão, que é o conhecimento generalizado do objetivo da recolha de dados, ou seja, voltamos à gestão da informação, ao pormenor, à granulidade dos dados. E este é um aspeto importante para percebermos políticas de proteção. Os atores que constroem esta informação não têm ainda estas preocupações, de definir isto. Cá está mais uma vez a importância da maturidade, na preocupação em manter a coerência da informação. Porque muito que era o passado dos sistemas clínicos, e com impacto na privacidade, a informação estava redundante em vários locais, correndo-se o risco de proteger de forma diferente a mesma informação. Porque num lado é consultada por um médico e num outro por um enfermeiro. Posso ter informação contraditória no mesmo processo clinico. Se depois eu vou aplicar algum tipo de privacidade, de acessibilidade a esta informação eu posso estar a induzir em erro. A nossa preocupação é que um item de informação, só esteja num local. E se existir em vários que seja atualizável e emigrável. Temos sempre a informação mais atual. Sobre isto é depois mais fácil aplicar regras de privacidade no acesso à informação.
P6.V2.1 – P3HFF#04	No dia-a-dia a verdade é que não questionamos muito o porquê da recolha de determinados dados. Muitas vezes só depois de termos dado ou recolhidos determinados dados, é que que colocamos a questão "para que é que isto é preciso?" Muitos inquéritos que muitas vezes recebemos dá para ver a imiscuidade na nossa esfera pessoal. Como é que chegaram aquela minha informação pessoal? No domínio da saúde deveria haver mais informação sobre o objetivo da recolha de dados, mais informação sobre responsabilidade na recolha de dados, porque sobretudo em termos de saúde pública existe uma coisa em que nós culturalmente não somos muito pródigos, que é aquilo que entendo como fazendo parte do exercício de cidadania, e de facto nós não exercemos essa cidadania de forma útil à sociedade em si. Quando respondemos a inquéritos de promoção da saúde, nos vimos isso. Nós tínhamos o dever responder a dados estruturados, bem identificados, para um objetivo, e depois deveríamos dar o retorno à população onde os dados foram recolhidos. Concordo que havendo um conhecimento maior sobre aquilo que é o objetivo da recolha de dados, a responsabilidade sobre a recolha de dados fica depois mais fácil compreender as políticas de privacidade aplicadas. Existe uma ligação direta. Há um retorno.
P6.V2.1 – P1SPMS#02	Sim concordo. Acho que é importante que estas questões sejam mais trabalhadas nas organizações, nomeadamente ao nível da gestão da informação. Descrever e compreender os processos de recolha de dados, qual é a justificação, tem que haver um maior conhecimento destas questões. Nós internamente tivemos a necessidades de implementar uma política de análise e extração de dados. Qualquer extração de dados que nós tenhamos que fornecer, por exemplo no suporte a um estudo, temos que enviar para o conselho de administração uma justificação, o âmbito, o objetivo, e qual é a informação que vamos fornecer, para depois ser analisado posteriormente. Temos esta preocupação.
P6.V2.1 – P2SPMS#03	Deveria existir um maior conhecimento. Facilitava depois aquilo que são políticas de privacidade e proteção de dados. Esta questão ao se tutelada e gerida por organismos diferentes, dificulta que se promova um maior conhecimento. Um hospital privado, quando faz um exame já pede este tipo de autorização. Um hospital público provavelmente não tem o mesmo nível de processo definido. No ato inicial de recolha da informação não é pedida de imediato a autorização para uso daqueles dados para determinados fins. Um hospital privado pergunta. Há aqui já uma diferença entre o que é privado e público, e porque é que um faz e o outro não faz.
P6.V2.1 – P2SPMS#04	Sim deveria haver um maior conhecimento. Nós aqui temos essa preocupação. Estamos a desenvolver políticas de utilização e cedência de dados. Cada pedido de dados que é feito tem de ser aprovado primeiro pelo conselho de administração, tendo em conta a sua criticidade. Deveria haver uma aposta maior ao nível da gestão da informação.
P6.V2.1 – P1HES#01	Sim as pessoas deveriam saber mais sobre o objetivo da recolha de dados. Os profissionais deveriam trabalhar mais a componente de gestão a informação. Olhar para os dados com outra atenção. Agora com os desafios diários que lhe são pedidos, e as tarefas diárias exigidas, tenho dúvidas que estes estejam abertos a trabalhar a gestão da informação.

	As pessoas hoje em dia debitam a informação para dentro dos sistemas de informação sem qualquer preocupação. Existem muitos processos em que não existe um conhecimento a 100% do porquê do registo daquela informação. Muitas vezes as pessoas questionam, porque estão obrigadas as registar aquilo e a fazer aquilo. Antes em suporte papel era muito mais fácil. Se tentarmos aplicar aqui políticas de privacidade a estes processos estas não vão ter sucesso. Pelo menos da forma como as coisas são agora.
P6.V2.1 – P2HES#02	Sim se na recolha de dados nos limitarmos a recolher a informação que nos faz falta e não recolher informação a mais é óbvio que vamos ter aqui uma maior facilidade ao nível da privacidade dos dados, até porque estamos a trabalhar com menos informação. Deveria haver mais gestão da informação, estudar e documentar mais os processos, o tratamento de dados. Admito que possam existir processos onde é recolhida informação a mais, nomeadamente através de alguns questionários que realizamos, como por exemplo o questionário que se preenche quando damos sangue. Ainda não são dados tratados de forma digital, mas para lá caminham.
P6.V2.1 – P2HES#03	É necessário conhecer a criticidade de cada processo. E depois é mais fácil identificar onde devemos ter mais cuidados de proteção. Existem dados mais críticos que outros, nomeadamente dados de análises clinicas, e a imagiologia. É dos processos mais críticos. Está disponível, muita informação sensível. E aqui é exigível uma maior preocupação para com a privacidade destes dados. Havendo um conhecimento sobre estes processos, mais críticos, depois é mais fácil a aplicação de medidas de proteção, de uma política de proteção.
P6.V2.1 – P3HES#05	Existe um grande desconhecimento sobre os objetivos da recolha de dados. Se as pessoas conhecessem o porquê da recolha de dados, com algum detalhe, facilitava depois a aplicação de algumas medidas de proteção. Quando num episódio, em suporte papel, se pedia os episódios anteriores conseguia-se dois ou três. Com toda a disponibilidade de informação que a gente tem hoje em dia, é completamente diferente.

P6.V3.1

P6.V3.1 – P1ULSNA#01	Seria sem dúvida. Mas não existe uma nomenclatura diretamente relacionada com a privacidade. Existe o senso comum, ou seja tudo o que se considera informação clinica considera-se informação sensível, obviamente terão os seus níveis de segurança. Dados administrativos, contabilísticos, da própria identidade da pessoas/utente acabam por ser considerados menos sensíveis, e qualquer profissional que lide com o utente terá capacidade de ver.
P6.V3.1 – P2ULSNA#02	Com toda a certeza. Identificação inequívoca de quem altera e lê os dados. Tendo várias organizações a utilizar e partilhar dados é necessário que elas entendam os dados da mesma maneira, que a linguagem seja comum.
P6.V3.1 – P2ULSNA#03	Sim. De certa forma existe esta classificação nas aplicações que temos, mais orientadas para níveis de acesso. No contexto de partilha, depende do que se queira partilhar. Estamos a falar de dados clínicos, dados demográficos. Faz sentido, haver uma nomenclatura, de forma ser mais fácil a partilha desses dados. É desejável existir uma nomenclatura partilhada por todas as organizações de saúde, permitindo por exemplo perceber quais os perigos da junção dos diferentes tipos de dados.
P6.V3.1 – P1USF#01	Sim é importante a existência de uma nomenclatura. Já existem diferentes níveis de acesso ao nível do utilizador, nomeadamente para médicos e profissionais de enfermagem. É importante que exista uma partilha desta nomenclatura para que a proteção seja o mais homogénea possível entre instituições.
P6.V3.1 – P2USF#02	Sou a favor das nomenclaturas. Tenho nomenclaturas para tudo. Quem estiver a trabalhar com as nomenclaturas sabe de certeza o que

	é aquilo, a que se referem e para que servem. Neste momento as aplicações são todas verticais, em que o acesso aos dados é apenas controlado com base no perfil do utilizador. Um médico por exemplo, não sendo o "dono" do processo clinico, ele tem que ver toda a informação do utente. Não vai ser fácil chegar a este ponto, a esta nomenclatura. Fazer esta camada, esta integração intermédia vai ser complexo. Dados de identificação do utente e dados administrativos são sempre partilhados. Ao nível dos dados do processo clinico é que faz sentido esta proteção e dados através de nomenclaturas, através da classificação de dados (…). Em determinadas situações a classificação dos dados pode complicar, por exemplo o consentimento.
P6.V3.1 – P1INEM#01	Sim facilitava, nomeadamente à equipa de IT. Facilitava a definição de perfis de acessos. Ou seja saberíamos que perante um determinado nível do utilizador, que dados lhe podemos dar. Existem níveis de autenticação, mas depois este controlo de acesso é relegado para as aplicações. Cada aplicação tem a sua forma única de gerir o acesso à informação, ou como é que trabalhamos essa informação. Esta classificação de dados para o domínio da colaboração deveria evoluir no sentido de definir os vários perfis ou camadas de dados, até onde podem ser partilhados, assim como a definição de dados que nunca podem ser partilhados. Existe um conjunto de dados, muito específicos que não devem ser partilhados. Facilitava a interoperabilidade entre organizações ou entre aplicações, e mesmo ao nível local – existe cada vez mais a necessidade de integração das aplicações umas com as outras, independentemente do fornecedor. Existe contexto para adotar ou pelo menos adaptar um *standard* neste domínio.
P6.V3.1 – P2INEM#03	Faria sentido uma nomenclatura neste aspeto. Se eu tivesse uma classificação que permitisse dar ou definir regras para aquilo que são dados sensíveis, era mais fácil. Poderia passar apenas pela adaptação de um *standard* a esta necessidade. Ao nível da partilha de dados entre organizações, tem que haver um grupo, ou alguma entidade que define e que apresente um *standard*, que seja cumprido por todos de forma homogénea. Caso contrário não se consegue definir políticas iguais para tratar a mesma coisa. Uma coisa, é por exemplo nós INEM definirmos um conjunto de regras e querermos inclusive incutir essas regras a outras entidade -estas aceitam ou não estas regras. Outra coisa é haver uma entidade reconhecida que possa definir *standards*, que defina políticas para todas as entidades que os queiram adotar.
P6.V3.1 – P2INEM#04	Sim. Neste momento não é uma prática comum a classificação dos dados, nem a utilização de um *standard* de classificação. Não é de todo fácil a sua implementação, seria necessário uma cultura diferente que penso que não existe. Não será muito fácil colocar uma nomenclatura a ser partilhada por todas as organizações e até mesmo dentro das organizações. Mas seria útil! Passar para todas as organizações este tipo de nomenclatura faria com que pudessem ser mais facilmente ajustadas a medidas de segurança. É uma ideia que terá que ser mais bem assimilada por todos nós.
P6.V3.1 – P2INEM#09	Sim, havendo uniformização é mais fácil a aplicação de políticas de privacidade aos dados. É necessário definir o que é importante classificar, e como classificar. Ou seja, o que é reservado, da esfera pessoal. Assim sempre que existe tratamento de dados, eles deveriam ser imediatamente classificados.
P6.V3.1 – P2INEM#10	Sim, se conseguíssemos ter uma nomenclatura, ficava muito facilitada a aplicação de políticas de privacidade. Passávamos a ter níveis de sensibilidade, o que facilitava a generalização das políticas. Poderia ter dados que durante a fase de utilização tinha uma categoria, mas quando passava para o armazenamento, tinha outra categoria. Teria sem dúvida uma adaptação muito mais dinâmica de políticas. Entre organizações, permitiria a garantia na semelhança dos processos de utilização e armazenamento de dados. Se isto for uma solução, significa que tem que haver uma partilha desta nomenclatura. Idealmente, as organizações têm que crescer como um todo.

	Estamos a partilhar dados, pelo que os meus dados têm que ter as mesmas medidas de proteção do outro lado.
P6.V3.1 – P1HFF#01	Concordo com a exigência diferenciada dos dados. Dai já termos falado em risco e criticidade dos dados, gestão da informação, análise de risco – sobre esta informação qual o grau de risco? No que toca à classificação de dados a ISO270001 já contempla várias sugestões quanto ao desenvolvimento de uma nomenclatura. Agora apesar da ideia, do interesse, da existência de um projeto a este nível, ainda não existe uma nomenclatura implementada. Uma nomenclatura facilitava certamente aquilo que são políticas sobre a passagem de dados entre organizações, em que era possível saber se esta informação estava sinalizada como informação critica ou não. Uma nomenclatura a este nível, generalizada nas organizações, facilitava a passagem de dados entre organizações nomeadamente através da classificação da sua criticidade, sensibilidade e segurança. Seria depois mais fácil a definição de requisitos a cada um dos níveis identificados.
P6.V3.1 – P2HFF#02	Sim uma nomenclatura iria facilitar a aplicação de políticas de privacidade. Em termos de segurança ainda não temos nenhuma nomenclatura aplicável. Tratamos todos os dados por igual. Esta nomenclatura deveria acompanhar o ciclo de vida dos dados, desde o registo até ao próprio armazenamento. Agora esta nomenclatura deve ser partilhada. Crescer como um todo. Existem instituições com mais experiência a este nível que outras. Todas as instituições são mais reacionárias do que proactivas. Algumas instituições já podem ter alguns procedimentos definidos.
P6.V3.1 – P2HFF#03	Eu julgo que sim. Esta nomenclatura existe, mas é ainda muito macro, que é capaz de não cumprir totalmente. Aquilo que muitas vezes existe depende daquilo que a prática clinica diz. Ou seja, aquilo que forem as orientações clinicas, porque muita da privacidade, no universo clinico, tem a ver com o que faz sentido ser consultado, por que ator e em que contexto. Isto é complexo, dou o exemplo dos mais comuns, o VIH, em que o diagnóstico é absolutamente crucial para qualquer profissional, pondo em risco a sua saúde e a do paciente, mas não é líquido, claro ainda quem deve ter acesso á informação do diagnóstico, no caso de um doente de infeciologia. Portanto, ainda há aqui estas questões de quem deve ter acesso, para depois aplicar as regras por cima. E depois, é necessário ter tudo isto muito estratificado. O que existe hoje é muito macro – temos informação da enfermagem, informação médica, ou informação médica de psiquiatria. Neste paradigma, então se é informação médica de psiquiatria, e existe um conceito de confidencialidade no processo clinico que faz com que só o próprio o veja. Isto, nós podemos padronizar, nós podemos dizer que esta avaliação é uma avaliação naquele contexto em que só o profissional que registar é que vê, apesar de ser um processo clinico transversal. Os outros médicos não veem este processo clinico. Agora a transferência de dados deveria depender à partida de uma padronização dos dados deste género. Nós temos dois tipos de transferência: entre sistemas dentro da mesma entidade, e entre sistemas de entidades diferentes. Que informação é que eu devo ir buscar por exemplo ao sistema de patologia, ao sistema de cardiologia, para colocar no repositório, porque eu à partida não tenho muita preocupação em saber quem é que a registou e quem lhe tem acesso, porque ao migrar estes dados para o meu sistema, de um forma estruturada, eu depois vou dar acesso a um conjunto de pessoas. Portanto, pessoas que se calhar naquele sistema, estavam restritas com acesso restringido, neste sistema já conseguem consultar dados. Estas preocupações não existem. Agora quando os dados passam para outro sistema, externo, um *metadado* pode transportar esta nomenclatura.
P6.V3.1 – P1SPMS#02	Estamos a falar de uma nomenclatura que permita dizer que estes dados exigem uma atenção especial? Que estes dados não são perigosos e podem ser partilhados? Sim uma nomenclatura destas seria bastante útil. Porque de certa forma também nos permite avaliar se temos que estudar um pouco mais a forma como estamos a divulgar determinada informação. Nós sabemos o quanto ela é crítica, se pode ser utilizada para outros fins, mas não temos como a classificar. Seria bastante útil uma sinalética que permitisse definir, não só o tipo de informação, mas

	também a questão de privacidade, se é ou não critica. Existindo uma ferramenta destas, acho que toda a gente deveria ter esta nomenclatura, no suporte ao desenho de sistemas. Ainda não estamos a utilizar uma nomenclatura destas. A única forma que temos e controlar o acesso aos dados é com base no perfil do profissional (*role-based*). Contudo ao nível dos sistemas locais é possível ocultar determinada informação para outros perfis ou outros profissionais. Neste caso pode-se manter a privacidade de determinados dados. Só o profissional que está a seguir o utente, num determinado processo ou caso, é que consegue visualizar determinado tipo de dados. Eu acho que é preciso trabalhar mais neste domínio, olharmos para os dados independentemente das aplicações, ter algo muito claro, orientações de como classificar informação com vários níveis de privacidade. Definir estas regras é sempre útil, aplicáveis a qualquer cenário de utilização de dados, assim como ter um vocabulário dentro da privacidade. A privacidade é aquele termo que dá para falar de muita coisa! No caso dos processos clínicos eletrónicos, nós podemos ter uma nomenclatura nacional, e sermos nós a classificar aqueles campos com um nível de privacidade, com proposta do ministério. A informação era classificada. Claro que a mesma ferramenta vai ter que existir também a nível local. Com uma categorização da informação nós poderíamos disparar um alarme quando a informação não está a ser utilizada de forma correta.
P6.V3.1 – P2SPMS#03	Se esta nomenclatura fosse um *standard* partilhado por todas as organizações, era depois mais fácil aplicar medidas de proteção. É passível haver uma classificação bastante simples em relação àquilo que é a sensibilidade dos dados, embora o conjunto de dados seja muito alargado. Tudo que seja, dados pessoais, identificáveis, dados que podem causar danos do ponto de vista moral, já limitava muito a sua utilização. Tem muito a ver com a identidade digital, apesar de serem matérias independentes. A questão é quem acede àquele tipo de dados é quem diz ser. Os mecanismos de autorização ficam facilitados. Era necessário definir mais os perfis. Ou esta nomenclatura se traduz naquilo que são normas, com base em normas internacionais, ou então não vejo por exemplo a SPMS, que é uma empresa prestadora o possa fazer. Somos uma empresa operacional. Só mesmo partindo de um *standard* internacional, uma ISO por exemplo, é que se conseguiria implementar este requisito. O ideal é que o acesso aos dados não fosse apenas condicionado pelo perfil do utilizador, mas também por esta camada intermédia de classificação de dados, que permitissem mais filtros em termos de visualização.
P6.V3.1 – P2SPMS#04	Se existisse uma nomenclatura de classificação de dados, que de alguma forma fosse partilhada pelas instituições, ficava facilitado aquilo que é a relação dos conjuntos de dados com os conjuntos de profissionais e não os dados como um todo. Acho que isto é urgentíssimo. Tinha que se envolver uma equipa, que estudo os dados por áreas, como dados administrativos, clínicos, contabilísticos. Para cada área envolver pessoas dos vários departamentos, com responsabilidade nestas questões. No fundo é criar um *standard*. Um dos grupos do CAIC pode desenvolver este trabalho. Quando os dados num sistema tiverem associados um determinado risco, e se depois passarem para outro sistema e tiverem o mesmo nível associado, então teremos um sistema eficiente em termos de proteção de dados. Os dados têm de ter o mesmo significado e valor em todo o lado, caso contrário temos políticas de proteção muito díspares. E agora vamos começar, com o EpSOS a trocar dados com a europa.
P6.V3.1 – P1HES#01	Os dados têm significados diferentes, valores e objetivos diferentes, sensibilidades diferentes. Tal como na gestão documental. Tenho algum receio de mais uma nomenclatura em saúde. Digo isto pelo que ouço dos médicos. Os médicos dizem que têm que ter um

	pensamento livre, que não podem basear-se apenas em nomenclaturas. Queixam-se por exemplo de eu ter o campo a ou o campo b, e de não poder fazer tudo em texto livre, pois dizer que têm um influência negativa naquilo que é o raciocino clinico e médico. Agora uma nomenclatura para de alguma forma poder classificar os dados para depois ser mais fácil aplicar políticas de privacidade, da responsabilidade dos responsáveis pelos sistemas de informação. Tenho dados em que o risco é maior. Tenho contudo várias aplicações e sistemas, o que faz com que exista muita dificuldade em homogeneizar aquilo que é políticas de privacidade. Apesar de acreditar que a aplicação de políticas de privacidade ser mais fácil, com base numa nomenclatura de dados, não estou a ver como é que depois isto é exequível numa malha desta dimensão. A informação que nós geramos todos os dias é muito grande. Não fazemos gestão da informação, fazemos apenas gestão de sistemas. Não olhamos para a informação, nada! Se começarmos a olhar para a informação provavelmente teríamos uma ideia completamente diferente sobre os conteúdos, sobre a informação. Precisamos é de ter profissionais a tempos inteiro, daí eu ter perguntado como? Havendo uma nomenclatura que pudesse ser partilhada, facilitava aquilo que é o propósito da partilha de dados. Eu posso decidir que determinado grupo de dados não são para partilhar. É quase querer escolher os campos que eu quero disponibilizar para a PDS. Hoje já fazemos uma mapeamento parecido através do perfil do utilizador. O médico vê determinada informação diferente da que um enfermeiro vê, mesmo que no mesmo processo. O mesmo acontece com os auxiliares, administrativos e técnicos de laboratório e raio x. O sistema controla os acessos dos utilizadores porque há classes de dados. Poderíamos pensar em políticas de privacidade com base nestas classes. Qualquer pessoa que queira ter um acesso a informação superior àquilo que são as funções que exerce legalmente, tem que solicitar este acesso ao conselho de administração e ter autorização da direção clinica. Isto no ALERT, mas se a informação passar para um outro sistema, provavelmente as classes já são outras e a utilização de dados é diferente. Nós aprendemos com esta política do ALERT que depois tentamos aplicar a outras situações. Não existe contudo uma norma, as coisas não escritas, não estão formalizadas. Os processos não estão formalizados.
P6.V3.1 – P2HES#02	Sim concordo que sim. Uma nomenclatura facilitava depois a aplicação de políticas de privacidade. Temos já vários casos que aplicam nomenclaturas de classificação de dados. Teria como efeito prático uma garantia de acesso seguro a essa informação. Ou seja, para um determinado nível de informação só podem aceder determinado tipo de profissionais. Todos os outros não iriam aceder aos dados. Isto feito de forma uniforme para a organização era o ideal.
P6.V3.1 – P2HES#03	Sim a adaptação de uma nomenclatura de classificação dos dados, facilitava depois a aplicação de medida de proteção destes dados. A proteção de dados seria mais focada, mais objetiva. A nomenclatura é também importante quando partilhamos dados com outras organizações. [...] Se nós tivéssemos já uma nomenclatura sabíamos já quais os níveis ou categorias de classificação dos dados, e eu sei que para um determinado nível eu tenho um conjunto de medidas. Se calhar é mais fácil eu saber que do outro lado para o mesmo nível também são garantidas as mesmas medidas. É mais fácil sem dúvida fazer este alinhamento. Esta nomenclatura tinha que ser igual para todos, tipo um *standard*. Uma norma que teria que ser respeitada por todos.
P6.V4.1	
P6.V4.1 – P2ULSNA#02	O que falamos há pouco, uma linguagem comum em proteção de dados. O próprio ministério da saúde ao aceder ás nossas bases de dados, nós não sabemos que tipo de informação é utilizada, não existe uma relatório desta utilização. É necessário alinhar a proteção de dados em todas as organizações e as medidas de acesso físico.
P6.V4.1 – P2ULSNA#03	A preparação para a partilha é preponderante, sem esta acaba por não haver partilha. Muito sinceramente a partilha de dados entre

	sistemas díspares, se eu fosse responsável por uma destas instituições não autorizaria a partilha de dados com alguém que não tivesse uma preparação prévia. São necessários meios humanos principalmente, a reunião das pessoas e a análise do que pretendem partilhar em concreto.
P6.V4.1 – P2USF#02	Primeiro é necessário um consenso sobre os dados e como os devemos começar a proteger. Com tanta organização, como é que se começa a proteger dados? Tecnicamente começo logo a pensar nos níveis de segurança, backups, firewall e o controlo de acesso aos dados. Se tivermos uma segurança das infraestruturas e em simultâneo uma segurança da informação asseguradas, teremos com certeza o cenário ideal. Teremos assim uma resposta boa do lado da infraestrutura, e do lado dos dados, garantias que cumprimos a normas de segurança, ou seja uma situação ideal.
P6.V4.1 – P2INEM#03	É complexo pensar como se pode fazer isto. Uma harmonização tecnológica pode facilitar em parte. Se tivermos standards, algo que todos consigam cumprir, melhor. Facilita sem sombra de dúvidas. Se houver um conjunto de regras que sejam comuns, *standards*, classificação de dados, facilita-se depois a privacidade como um todo.
P6.V4.1 – P2INEM#04	É uma pergunta difícil. Tudo isto que pergunta é um assunto que merece uma grande reflexão. A tecnologia é preponderante, quanto mais desenvolvimento tecnológico mais garantias para a proteção de dados. Deveria haver uma maior prática na utilização de standards, por exemplo ao nível da segurança, ao nível de desenvolvimento de interfaces, para garantir determinados níveis de qualidade.
P6.V4.1 – P2INEM#09	É necessário em primeiro saber quais é que são os dados que para a saúde no seu todo, podem ser tratados e como devem ser protegidos. Independentemente dos sistemas serem diferentes, esta partilha de dados está muito dependente da tecnologia, devendo existir de algum modo alguma harmonização tecnológica. Cada organização cria as suas bases de dados com base nas suas necessidades, e por vezes é difícil esta harmonização face à diferença tecnológica. A interoperabilidade está a ajudar, mas por vezes pode não ser fácil. É necessário objetivos comuns entre todas as organizações a este nível [privacidade dos dados].
P6.V4.1 – P2INEM#10	É uma pergunta muito complicada. Em primeiro, acho que o se deveria começar por sensibilizar as pessoas. É o ponto fulcral. É necessário que as pessoas tenham noção da forma com que lidam com os dados. Para operacionalizar esta questão, é necessário também pensar-se na integridade tecnológica e de seguida na forma de partilha de dados. Havendo a presença de um *standard* para estas questões, melhor ainda, assim como uma nomenclatura de classificação dos dados. É necessário que as pessoas não contornem o risco. Tudo isto só funciona se for eficaz, controlado, otimizado de forma continua. É necessário reduzir os riscos de intrusão, de perdas de dados, ou outros riscos. O facto de haver várias organizações envolvidas, tem que haver um grupo que dinamize estas questões, que verifique as dificuldades que cada entidade tem, e eventualmente apresentar soluções para as ultrapassar. Muitas vezes a solução passa pela partilha [de experiências].
P6.V4.1 – P2HFF#02	A partilha de dados cada vez mais vai ser uma realidade. A eficiência dos sistemas e das organizações começa a depender desta partilha. Criar linhas orientadoras que nos permitam orientar nas várias camadas. Ao nível da segurança as tecnologias aplicáveis são preponderantes, sendo que a interoperabilidade técnica a este nível é cada vez mais facilitada. Os próprios sistemas já trazem mecanismos de segurança implementados. Passando da camada técnica para cima é importante haver *standards* que de alguma forma facilitem a colaboração, haver um conjunto de padrões – padronização das melhores práticas de segurança (ao nível da rede já temos algumas indicações da RIS, mas não temos ao nível dos sistemas), requisitos para um sistemas seguro, uma taxonomia. A proteção e dados por vezes tecnicamente é muito simples de implementar, só que não é feita devido ao impacto causado, que mesmo sendo mínimo, provoca uma demora na implementação do projeto. Quem decide, ao nível da gestão, deve compreender que é importante

	haver proteção de dados. Fazer uma proteção mais focada nos dados e não tanto nas infraestruturas.
P6.V4.1 – P2HFF#03	Nós nunca vamos conseguir otimizar esta dependência se não tivermos informação de forma estruturada. Neste momento temos muitos hospitais a organizar a sua informação de maneiras muito distintas, o que complica depois um processo de segurança, e tipificação com a semântica da proteção de dados. Ou seja o 1º requisito é ter uma estrutura de dados, bem tipificada, saber-se que uma nota de alta tem que ter aquela informação, é acedível por estes atores, por exemplo. Os objetos que constituem a informação do processo clinico deveriam ser claros. A heterogeneidade tecnológica já não é um considerando muito forte. A partir do momento em que eu tenho informação estruturada, e hoje já existem modelos informáticos para ter um repositório estruturado, e eu consigo transacionar informação mediante uma tipificação, um *layout* bem definido, eu só tenho que acrescentar alguns parâmetros de categorização da informação. Se eu poder categorizar esta informação, quem a recebe sabe quem deve ter acesso a ela e que perfil de acesso a pode utilizar. Nós ainda não estamos a este nível. O nível ainda é, 1º ter a certeza que temos a informação de forma estruturada e correta, para depois a poder classificar. Tecnicamente ainda não estamos num nível superior, a esta altura, porque temos motores de interoperabilidade, temos motores que fazem toda a rastreabilidade da transação. Já conseguimos saber isto dentro do nosso hospital. Mas com o exterior não conseguimos saber. Mas podemos ter algum motor agregador, por região por exemplo, que faça este trabalho, mais do que dar ligações ponto-a-ponto. No futuro nós temos que caminhar para uma privacidade focada nos dados e não apenas nas infraestruturas. Já falamos disto.
P6.V4.1 – P2SPMS#03	Não é fácil, até porque o conceito como diz, o que separa o que é privado e é público não é igual para toda a gente. Nas redes sociais, muita gente pública informação pessoal para um universo desconhecido. A informação do fórum clinico, e quando são usados dados que já não são para os fins diretos e que são para aplicações terceiras, ou que são usados por outros profissionais que não os que recolheram os mesmos. A camada de segurança já é muito uniforme em termos nacionais, é já muito equivalente. As tecnologias utilizadas são muito comuns. A proteção e a privacidade deveriam ter o mesmo nível de entendimento. Um *standard* a este nível ajudaria certamente. Existem vários mecanismos de autorização. Necessitamos de um mecanismo comum, aceite por todas as partes de autorização. Porque a privacidade é isto mesmo. É necessário ver em que contextos os profissionais podem ver a informação. Podemos mover uma proteção centrada na segurança para uma proteção centrada no cidadão. Ele é que sabe se quer ou não dar os seus dados para a aplicação a, b, ou c. Mesmo para cidadãos que não tenham facilidade em dar o seu consentimento, já temos mecanismos interessantes que podem facilitar esta tarefa. Basta verificar o cartão de cidadão e da integridade do certificado. A autorização é a existência materializada do cartão. Obriga a que seja explicado à pessoa – preciso do seu cartão para aceder aquele sistema, isto é o seu veículo de autorização.
P6.V4.1 – P2SPMS#04	Ao nível dos centros de saúde os sistemas de informação já são mais homogéneos, ao contrário dos hospitais. Estamos muito dependentes das tecnologias. São necessárias normas, regras que ajudem as pessoas a desenvolver esta dependência. Mesmo nos centros de saúde temos 4 ou 5 sistemas clínicos instalados, em que as coisas são feitas de maneiras diferentes. Nuns, os médicos registam os dados e ainda têm um período para alterar estes dados, mas noutros alteram os dados quando estes querem. Outros por exemplo guardam todas as alterações registadas, e não apenas a última alteração. Isto é importante quando é necessário provas para um determinado processo de auditoria.
P6.V4.1 – P2HES#02	Tem a ver com os critérios uniformes. Ou seja, tem que haver uniformidade em todas as organizações que irão colaborar. Com sistemas homogéneos tudo iria trabalhar muito melhor. Iriamos diminuir muitos riscos, tanto ao nível da segurança como ao nível das interfaces. E ao mesmo tempo a monitorização da aplicação desses critérios uniformes - se estão a ser aplicados, se estão a ser bem aplicados e o que podemos melhorar ou não. Se não existirem muitos pontos de falhas podemos caminhar para uma otimização. Caso

	contrário com os pontos de falhas que existem, com a quantidade de sistemas que existem, caminhar para uma otimização, uma uniformização é difícil. Uniformização diz respeito à utilização de *standards* que permite que todos trabalhem da mesma maneira. Ao nível da segurança os *standards* são uma realidade. Com base num *standard* é depois mais fácil definir um conjunto de medidas de segurança. Teríamos também de perceber que standards podemos aplicar à proteção e dados para melhora esta otimização. A privacidade tem que caminhar em dois sentidos: para o lado dos dados e para o lado das infraestruturas, porque se fizermos só a análise de dados um ataque à infraestrutura pode colocar em causa a privacidade daqueles dados. Neste momento a maior concentração é ao nível das infraestruturas, no patamar da segurança.
P6.V4.1 – P2HES#03	Neste momento o protocolo de comunicação de dados entre aplicações, internamente, é o HL7. Para passar dados para outras instituições teria que ser algo idêntico, de preferência encriptado. [...] É necessário um *standard* que permita a passagem de informação entre sistemas. Um *standard* que permite segurança. Se alguém apanha o ficheiro não consegue identificar a pessoa a que diz respeito. Em termos de segurança de infraestruturas não estamos mal, apesar de margem de evolução, já cumprimos com os mínimos. Em termos de proteção de dados existe mais margem para evoluir neste sentido.

2. *Data Reduction*

P6.V1.1	**Compreensão das limitações** São conhecidas as limitações da utilização e partilha de dados para o ambiente de colaboração?	**Forma de atuar.** Como atuam as organizações. A que nível se traduz esta dificuldade? Como gerem estas situações? Qual a preocupação para com os dados?
Padrão encontrado Conhecimento insuficiente Falta de informação	"Não me parece, acho que não estão cientes. Ainda continua a existir muito a tradição de trabalhar com aquilo que é meu, e não de haver esta partilha." (P6.V1.1 – P1ULSNA#01)	"De certa forma as pessoas depois de obterem os dados, de certa forma têm a ideia que podem fazer tudo o que querem com esses dados." (P6.V1.1 – P1ULSNA#01)
	"[…] na sua forma mais abrangente não existe uma clareza muito bem definida em relação a isto. Existe uma clareza muito grande na área da segurança […]" (P6.V1.1 – P2ULSNA#02)	"Mas olhar para os dados em si como um universo paralelo à segurança física, acho que não existe essa noção. Em relação a este conceito que é transversal a todas as instituições, e que se tem vindo a arrastar no tempo, […], as pessoas acham que desde que o meio físico esteja protegido está tudo bem, os dados foram sempre descartados para segundo plano." (P6.V1.1 – P2ULSNA#02)
	"[…] mas não suficientemente conscientes sobre esta questão. Há sempre situações que têm que ser colocados à comissão nacional de proteção de dados." (P6.V1.1 – P2ULSNA#03)	"Veja-se o caso em que as pessoas partilham dados através de meios que não são institucionais." (P6.V1.1 – P1USF#01)
	"Para a troca de dados com outras organizações existe uma consciência sobre os limites e regras de utilização." (P6.V1.1 – P2ULSNA#03)	"No nosso caso, na saúde, e com a validação da CNPD, todos nós temos preocupações com os dados. Todos temos obrigações para cumprir." (P6.V1.1 – P2USF#02)
	"Estão cientes até certo ponto. Não estão bem cientes daquilo que pode acontecer caso as coisas corram mal. Não pensam muito nestas questões." (P6.V1.1 – P1USF#01)	"Deveria haver uma maior informação sobre as tarefas que podemos fazer em relação aos pessoais, o que não podemos fazer. Existe uma necessidade em saber os cuidados a ter com dados sensíveis." (P6.V1.1 – P3USF#03)
	"Eu acho que há algumas organizações que até estão. É um assunto, que se não é atual, é um assunto muito falado. Começa a ser um aspeto muito cultural. Depende muito da preparação organizacional para estas matérias." (P6.V1.1 – P2USF#02)	"Os limites que nós conhecemos poderão não ser os ideais. Penso que é uma questão em que as pessoas não estão muito sensibilizadas, em relação ao que pode acontecer depois dos dados estarem registados no sistema. Existe aquilo que nos foi incutido, é uma coisa ética, de como profissionais de saúde guardar sigilo em relação aos dados." (P6.V1.1 – P3USF#04)
	"Acho que neste domínio falta formação. […] À partida, e com base na nossa formação sabemos mais ou menos os nossos limites, mas podemos cometer erros. Era importante haver uma maior sensibilização, mesmo cultura." (P6.V1.1 – P3USF#03)	"Esta maior atenção na importância dos dados, desperta um maior interesse pela sua segurança." (P6.V1.1 – P3USF#06)
	"As limitações podem não estar bem presentes, estão presentes de uma forma relativamente empírica. Aprofundar o conhecimento sobre esta temática seria importante." (P6.V1.1 – P3USF#04)	"Porque, por exemplo o nosso caso, em que cada vez mais utilizamos dispositivos móveis, e alguns com dados sensíveis, em que é necessário uma noção clara do que se pode fazer. Existe muito trabalho a fazer nesta matéria." (P6.V1.1 – P1INEM#01)
	"Não, há muita falta de informação e de conhecimento nesta matéria." (P6.V1.1 – P3USF#06)	"Nós próprios não estamos e temos que pedir pareceres à CNPD para saber o que é que eles têm a dizer sobre a utilização de um determinado programa ou de um determinado produto." (P6.V1.1 – P2INEM#03)
	"[…] as pessoas têm algum conhecimento sobre o que podem fazer com os dados, mas não sei se será suficiente. Têm algum conhecimento sobre os limites." (P6.V1.1 – P3USF#06)	"As organizações de um modo geral, pensando neste caso apenas [na área] da saúde, cada organização, ou cada grupo de organizações, com realidades de utilização de dados distintas […], têm uma coisa em comum – a intensidade na utilização de dados." (P6.V1.1 – P2INEM#09)
	"As organizações estão sensíveis, agora se isso acontece como o desejaríamos, se calhar não." (P6.V1.1 – P1INEM#01)	"Como as realidades [de utilização de dados] são diferentes, as pessoas vão reagindo com base naquilo que lhes vai acontecendo, e não há uma planificação prévia, ou um estudo prévio que diga em relação aos dados, quais os limites. […]" (P6.V1.1 – P2INEM#09)
	"Não me parece que estejam hoje em dia. Mesmo que algumas, embora tenham preocupações e possam demonstrar essas preocupações, creio que não estão totalmente a par de tudo." (P6.V1.1 – P2INEM#03)	"[…] existe uma grande preocupação em relação à confidencialidade dos dados que temos em nossa posse. Mas sei que existem muitas organizações em que qualquer pessoa utiliza os dados. Não existe a preocupação com a proteção dos dados." (P6.V1.1 – P2INEM#10)
	"Acho que a maior parte não." (P6.V1.1 – P2INEM#04)	"O grande dilema é – temos certa informação que sabemos que se for partilhada pode trazer benefícios, em outras situações pode comprometer." (P6.V1.1 – P3INEM#06)
	"Eu acho que não." (P6.V1.1 – P2INEM#09)	
	"Penso que não. […] Mas as organizações não estão cientes das reais necessidades e dos reais problemas que têm. Assim como dos limites que têm, quando têm dados." (P6.V1.1 – P2INEM#10)	
	"Existe uma consciência destes limites. […] Temos consciência que é	

	necessário uma atenção especial nos dados." (P6.V1.1 – P3INEM#05)	"É necessário mais informação sobre direitos e deveres no que toca à utilização de dados." (P6.V1.1 – P3INEM#06)
	"Não. As pessoas não conhecem os limites. Eu próprio tenho alguma dificuldade, em algumas situações, de perceber até onde se pode ir." (P6.V1.1 – P3INEM#06)	"À partida as organizações só se preocupam em recolher informação, e só depois se preocupam a em a proteger. Isto está virado ao contrário. Deveria pensar-se antes em como manter a informação sigilosa. Deveria haver uma maior atenção em relação aos dados que se recolhem, como são utilizados." (P6.V1.1 – P3INEM#07)
	"Não. Não é a sua postura." (P6.V1.1 – P3INEM#07)	"[…] existe a comissão de informação clinica, em que situações de envio de informação para o exterior são analisados." (P6.V1.1 – P1HFF#01)
	Acho que não." (P6.V1.1 – P1HFF#01)	"Em relação à partilha de dados com outras organizações são levantadas sempre questões. Porquê estes dados? Porque estamos a partilhar estes dados? Qual o objetivo da partilha destes dados?" (P6.V1.1 – P2HFF#02)
	"Não, porque toda a gente dentro do hospital pensa que está debaixo de um "guarda-chuva" de privacidade, pelo facto de trabalhar para o hospital. […] Sabemos que existem alguns limites. Agora o conhecimento destes limites é que não é muito claro." (P6.V1.1 – P2HFF#02)	"Deveria haver um maior conhecimento partilhado sobre os limites relacionados com a partilha de dados entre organizações, nomeadamente através da PDS." (P6.V1.1 – P2HFF#02)
	"Não sei se estão cientes. Mas se estão cientes não fazem nada. O mais certo é terem outro grau de preocupação." (P6.V1.1 – P2HFF#03)	"E portanto tudo o que toca com privacidade nesta altura é indutor de barreira. Quando se quer que os clínicos adiram à PDS, falarem em mais esforço por causa da privacidade pode ser indutor de barreiras." (P6.V1.1 – P2HFF#03)
	"Eu não tenho dúvidas que as organizações não estão a ser proactivas, […] " (P6.V1.1 – P2HFF#03)	"Muitas vezes estas questões funcionam pela ocorrência. Eu não tenho dúvidas que num futuro próximo, algumas destas questões vão-se colocar de forma muito premente por razões legais." (P6.V1.1 – P2HFF#03)
	"Não estão cientes. Podem ter subjacente no seu dia-a-dia esta noção, mas porque efetivamente, não existe, tanto quanto eu sei, nas organizações, nenhum grupo ou comissão que tenha como missão dentro da organização ser o orquestrador de tudo isto. Não temos de facto a consolidação destes conceitos em si." (P6.V1.1 – P3HFF#04)	"Só por fatores exógenos, e no sector da saúde a mudança tem acontecido exclusivamente por fatores exógenos. De uma forma endógena é raro as coisas acontecerem." (P6.V1.1 – P2HFF#03)
	"Na colaboração com outras organizações a noção do que podemos ou não partilhar não existe. É necessário um maior conhecimento coletivo destas questões, e sobretudo algumas orientações." (P6.V1.1 – P3HFF#04)	"É necessário explicar de uma forma clara quais são os limites. É também uma questão de ética profissional." (P6.V1.1 – P1SPMS#02)
	"A maior parte das instituições tem algumas noções mas não uma visão clara de todas estas questões. Em relação à partilha de dados, nomeadamente através da PDS, os profissionais necessitam de ser melhor esclarecidos." (P6.V1.1 – P1SPMS#02)	"Existem ainda hoje casos em que as pessoas têm a noção que podem fazer tudo com os dados." (P6.V1.1 – P2SPMS#03)
	"Tipicamente quando um produto chega a uma instituição, está dá início à sua utilização. Não está consciente sobre as limitações que tem em relação à sua utilização." (P6.V1.1 – P2SPMS#03)	"Como é que a gente consegue dizer que estes dados são críticos e só devem ser vistos pelos psiquiatras, se não tiver uma classificação?" (P6.V1.1 – P2SPMS#04)
	Devem ser poucas as organizações que estão cientes. Existe muito trabalho a fazer." (P6.V1.1 – P2SPMS#04)	"Mesmo em relação à partilha dos dados, acho que as pessoas não estão cientes do risco. Cada um de nós sabe, mas por bom senso, e não porque alguém nos disse ou informou. Não existe nenhum "manual" ou regras definidas. O que pode ou não ser partilhado é assim decidido com base no bom senso." (P6.V1.1 – P1HES#01)
	Em relação à recolha e à utilização de dados acho que as organizações não estão cientes dos limites. Em relação ao que podem recolher têm imensas dúvidas.	"Não conhecem os princípios de proteção de dados. Mesmo aos sistemas de informação são pedidos dados que colocam em causa os princípios de proteção e dados, e que nós muitas vezes recusamos responder. Muitas vezes nem tem a ver com a cedência de dados mas com a filtragem de dados dentro de uma base de dados. Que não se pode fazer." (P6.V1.1 – P1HES#01)
	Alguns grupos profissionais têm algumas noções destes limites. Outros grupos nem tanto." (P6.V1.1 – P1HES#01)	"Normalmente quando surgem dúvidas recorremos à CNPD. Internamente, não temos um especialista em proteção de dados. Em algumas questões valemos também do gabinete jurídico. Em privacidade dos dados o próprio jurista tem limitações. Para os sistemas de informação as leis são mais específicas. Dependem de um conhecimento específico em sistemas de informação." (P6.V1.1 – P2HES#02)
	"Eu acho que ainda não estão bem cientes. Ainda há muitas limitações na parte decisora, de quem está à frente das instituições. Tendo algumas limitações, não recorrem a quem ainda possa ter algum conhecimento, no sentido de ajudar quando surgem dúvidas. Tentar perceber o que podemos ou não desenvolver. Que riscos é que podemos ter. Normalmente alguns dos decisores não têm esse conhecimento, não quando há dúvidas não procuram soluções." (P6.V1.1 – P2HES#02)	"Deveria ser claro, onde registar, em que sitio, em que local, o quê, e o que posso partilhar ou não. Autorizo ou não a partilha. O que interessa mais partilhar é o diagnostico, e se calhar é aquele que a pessoa não quer partilhar. São dados mais confidenciais." (P6.V1.1 – P3HES#05)
	"Penso que não estão o suficiente. O medo de acontecer alguma coisa [das consequências] é que ajuda a evitar certos problemas. […] Neste momento não existe uma noção clara do que podemos partilhar." (P6.V1.1 – P2HES#03)	

	"Acho que as pessoas têm consciência de que é limitado o que estão a recolher. Têm ideia que existe uma fronteira, pouco clara. As pessoas não refletem muito sobre isto." (P6.V1.1 – P3HES#05)	

P6.V1.2	Opinião sobre a globalidade do ciclo de vida dos dados Opiniões que consideram que todas as fases do ciclo de vida dos dados são preocupantes em matérias de privacidade dos dados.	Opinião específica para determinada fase do ciclo de vida dos dados. Apesar de considerarem todo o ciclo de vida dos dados preocupante, consideram algumas fases mais preocupantes e que justificam medidas adicionais de proteção.
Padrão encontrado Medidas específicas	"No meio digital as questões da privacidade surgem muito na fase de criação e utilização de dados e começam a surgir maiores preocupações na transferência de dados. O armazenamento e arquivo hoje estão mais ligados a questões de segurança." (P6.V1.2 – P1ULSNA#01)	"A destruição é fundamental. Era fundamental quando se utilizada arquivos em suporte papel, por forma a garantir a privacidade da informação" (P6.V1.2 – P1ULSNA#01)
	"Fazem todas parte do mesmo processo. Basicamente os dados são gerados, e até alguém os destruir ou apagar, eles vão existir, seja em meio físico, em papel ou em digital." (P6.V1.2 – P2ULSNA#02)	"A nossa concentração é a criação e utilização dos dados, nomeadamente na unificação de processo de pessoas mal identificadas, que geraram processos paralelos." (P6.V1.2 – P2ULSNA#02)
	"Existem várias fases, dependendo do tipo de dados [...].Há fases que são sempre preocupantes. Por exemplo a fase da destruição de dados tem que ser garantida, segura e validada. É uma fase crítica e preocupante. Claro que o armazenamento de dados é muito importante, em que é necessário assegurar que os dados que temos estão seguros e devidamente utilizados. Os dados em produção têm que ter garantias de utilização correta." (P6.V1.2 – P2USF#02)	"Este processo em papel, têm regras para a sua destruição. Nos dados digitais não temos esta preocupação." (P6.V1.2 – P2ULSNA#02)
	"Não vejo uma fase que seja mais preocupante (...). É a cultura da privacidade que tem que cobrir estas fases todas." (P6.V1.2 – P3USF#03)	"A transferência principalmente. [...] quando existe uma transferência, nós temos que perceber o que é que vai ser transferido." (P6.V1.2 – P2ULSNA#03)
	"Acho que acabam por ser todas muito importantes. Se a preocupação em relação à privacidade pode ser comprometida em qualquer uma dessas etapas, não é muito inteligente protegermos uma ou outra etapa e comprometer outras." (P6.V1.2 – P3USF#04)	"A criação e utilização não é muito uma preocupação porque, e neste caso em relação aos dados dos utentes, para as aplicações que nos chegam, não concebidas por nós, normalmente limitamo-nos a preencher dados que as aplicações nos pedem." (P6.V1.2 – P2ULSNA#03)
	"Eu acho que todas as fases devem contemplar medidas. Preocupamo-nos, hoje em dia, muito com a transferência, mas todas as outras fases são preocupantes." (P6.V1.2 – P3USF#06)	"No arquivo e destruição não temos muito essa sensibilidade." (P6.V1.2 – P2ULSNA#03)
	"Todas as fases são preocupantes, mas a destruição de dados pode ser uma das mais preocupantes." (P6.V1.2 – P1INEM#01)	"A utilização é uma das fases mais importantes. Os dados do utente nunca são destruídos. Os dados permanecem nos sistemas, nas bases de dados, mas deixam de estar acessíveis, existem alguns condicionamentos no acesso a estes dados." (P6.V1.2 – P1USF#01)
	"O facto de termos os dados armazenados quase indefinidamente, há que pensar na mesma em todas as fases. Os dados não se alteram quanto à sua confidencialidade, tenham eles o tempo que tiver." (P6.V1.2 – P2INEM#03)	"A transferência de dados, os sistemas começarem a utilizar os dados uns dos outros, que é aquilo que a PDS faz, preocupa-me, essencialmente porque [...] podem existir situações de exposição dos dados." (P6.V1.2 – P1USF#01)
	"Penso que todas as fases têm que ser pensadas como um todo, são todas muito importantes." (P6.V1.2 – P2INEM#04)	"Na maioria das vezes não damos a devida importância à destruição. A partilha de dados começa a preocupar as pessoas." (P6.V1.2 – P1INEM#01)
	"Sim todas estas fases justificam medidas de proteção para os casos em que se lida com dados identificáveis. Quando não se consegue associar dados a pessoas, o risco não existe. Ou seja, isto será tão mais importante quanto mais houver ligação de dados a pessoas." (P6.V1.2 – P2INEM#09)	"O manter os dados quase eternamente, é algo que eu questiono – deveria pensar-se seriamente na destruição de dados." (P6.V1.2 – P2INEM#03)
	"As fases iniciais, as de registo e utilização, são as mais preocupantes, mais criticas, mais sérias, em que os dados estão disponíveis à generalidade dos utilizadores. [...] Quando se chega a fase de armazenamento, os dados só já estão disponíveis a um grupo restrito de pessoas. Os dados nesta fase estão bastante protegidos." (P6.V1.2 – P2INEM#10)	"Claro que os dados que estão em utilização são os mais sensíveis. Do ponto de vista técnico é o mais difícil. São mais as circunstâncias em que pode haver violação de dados.
	"Todas são preocupantes. Em algumas tem que se ter uma particular atenção. Na criação deve ser questionado se posso ou não recolher estes dados. Na utilização tem de se perceber para que se quer os dados e que	"Naquilo a que eu me habituei a informação não deverá nunca ser destruída. A transferência de dados será sempre uma preocupação e têm vindo a aumentar." (P6.V1.2 – P2INEM#04)
		"Quanto à destruição de dados, é muito difícil deitar informação "fora". Agora deve ser cumprido o prazo de vida dos dados." (P6.V1.2 – P2INEM#10)
		"Penso que sim, algumas fases requerem mais atenção que outras. O arquivo por exemplo." (P6.V1.2 – P3INEM#05)
		"Em relação à transferência de dados entre instituições existe por parte das pessoas uma confiança inicial, que resulta do facto de lhes ser explicado que existe uma garantia e uma importância no que está a acontecer." (P6.V1.2 – P3INEM#05)
		"Normalmente não nos preocupamos com a destruição. Normalmente não existem normativos, sensibilidade, porque o pensamento que existe é que "é mais importante que um dado exista do que não exista". (P6.V1.2 – P1HFF#01)

dados é que se vão ser usados. Na mesma forma tudo o que transmito ou partilho a outro tem que ser nesta perspetiva. O armazenamento e arquivo são importantíssimos, mais que a fase de destruição. É importante que estejam bem armazenados, bem arquivados. Agora há dados que têm que obrigatoriamente ter um limite de utilização. E ai a forma como são destruídos é preponderante." (P6.V1.2 – P3INEM#06)	"Agora são necessárias medidas específicas para a utilização destes dados." (P6.V1.2 – P1HFF#01)
"De uma forma genérica todas estas fases deveriam ter uma atenção específica. Mas a armazenagem e destruição deveriam ter uma atenção especial." (P6.V1.2 – P3INEM#07)	"Quanto à destruição de dados, nós não destruímos dados, mesmo que administrativos. [...] Deveria isso sim haver algumas regras de proteção destes dados. É necessário uma preocupação a este nível." (P6.V1.2 – P2HFF#02)
"Todas elas deveriam ter medidas específicas. Há umas que preocupam mais, nomeadamente o armazenamento, transferência e o arquivo. Na criação e utilização nem tanto, apresar de ser previstas algumas medidas, nomeadamente na análise de que dados necessitamos, se são supérfluos." (P6.V1.2 – P2HFF#02)	"Nós também não temos nenhuma orientação sobre como destruir, passar para um 2º plano, digamos assim, em *offline*, acessível mas num contexto mais complexo." (P6.V1.2 – P2HFF#03)
"Hoje em dia esta janela temporal tanto quando eu sei é infinita." (P6.V1.2 – P3HFF#04)	"Muita informação com o tempo perde contudo interesse clinico. Esta informação pode permanecer no sistema, uma vez que pode vir a fazer falta, mas deve passar para uma *data warehouse* e estão lá, são acessíveis na mesma, mas não estão é naquele *front-end* quando o médico tem que tomar uma decisão. Tem a ver com a qualidade da estrutura de dados. Se os dados forem bem estruturados é fácil eu estipular regras e poder padronizar." (P6.V1.2 – P2HFF#03)
"Todas estas fases são preocupantes. [...]. Em termos de privacidade dos dados todas estas fases do ciclo de vida da informação importantes." (P6.V1.2 – P1SPMS#02)	"Havendo regras de privacidade também para a situação do arquivo e eliminação, têm que ser criadas exceções para situações como a que lhe apresentei." (P6.V1.2 – P3HFF#04)
"Eu diria que todas elas devem ser preocupantes em termos de privacidade." (P6.V1.2 – P2SPMS#03)	"Tipicamente, não conheço nenhum projeto na saúde que se preocupe com o arquivo, em termos de histórico da informação." (P6.V1.2 – P2SPMS#03)
"A informação em papel representava um risco menor em termos de privacidade do que um dado eletrónico. A privacidade dos dados só se coloca com esta facilidade de acesso dos meios tecnológicos." (P6.V1.2 – P2SPMS#03)	"Não existe sequer o conceito de destruição de dados. As nossas bases de dados têm "*terabytes*" de 20 anos, de mais fácil acesso." (P6.V1.2 – P2SPMS#03)
"Em termos da proteção da privacidade, temos um problema cada vez mais grave dado o aumento do volume de informação, em que acedemos a milhões de registos." (P6.V1.2 – P2SPMS#04)	"Andamos a tentar fazer com que alguns dados passem a dados históricos. A questão é, o que é que vamos passar?" (P6.V1.2 – P2SPMS#04)
"De uma forma diferente são todas importantes. Todas elas são importantes. Sendo que a utilização e a transferência são onde recaem as maiores preocupações. Uma má utilização é sem dúvida mais preocupante. Sobre o arquivo e destruição, os dados, mesmo no setor da saúde, não devem ficar eternamente nos sistemas. Mas nós temos. Nós não apagamos nada." (P6.V1.2 – P1HES#01)	"E começa a ser crítico por já não temos capacidade de disponibilidade destes dados nas bases de dados. Deveríamos pensar no arquivo e mesmo na própria destruição e dados." (P6.V1.2 – P2SPMS#04)
"A velocidade de evolução dos sistemas de informação não foi acompanhada pela legislação em proteção de dados." (P6.V1.2 – P1HES#01)	"É necessário definir o tempo em que os dados ficam no sistema principal, e contemplar as situações em que temos que fornecer dados ao exterior, como pedidos vindos do tribunal sobre determinado processo clinico." (P6.V1.2 – P2SPMS#04)
"Em matérias de privacidade eu acho que as mais preocupantes têm a ver com a utilização, transferência e armazenamento. Quanto ao arquivo, e que eu tenha conhecimento, nós não fazemos destruição de dados." (P6.V1.2 – P2HES#02)	"Sempre que a informação for vital e importante deve ser mantida nos sistemas. Temos que pensar em medidas específicas. Agora surge a questão – quem é que define estas medidas específicas?" (P6.V1.2 – P1HES#01)
"Todas estas fases são preocupantes, em matéria de privacidade dos dados. Claro que os dados mais recentes são mais preocupantes. Dados em arquivo, com mais de 5 anos, também são preocupantes, mas não como os dados em utilização. São contudo fundamentais à história clinica do utente." (P6.V1.2 – P2HES#03)	"A proteção dos dados em arquivo deve permitir a identificação da pessoa, por forma a poder fazer uma reconstituição ou suportar um estudo sobre a família em causa." (P6.V1.2 – P2HES#02)
	"Não temos medidas específicas para destruição de dados. Medidas de privacidade não são ainda implementadas." (P6.V1.2 – P2HES#03)
	"A criação é o mais crítico. É o momento para o qual muitas pessoas ainda não perceberam que um registo de diagnóstico pode ser essencial para o utente daí a 5 ou 6 anos." (P6.V1.2 – P3HES#05)
	"Os dados da saúde não podem ser eliminados. Temos os sistemas subcarregados de informação. Anualmente estes registos deveriam ser transferidos do ativo para o inativo, tipo armazenamento." (P6.V1.2 – P3HES#05)

P6.V2.1	Conhecimento sobre os dados Os profissionais devem apresentar uma maior compreensão sobre os dados e os processos de tratamento? A privacidade deve ser desenhada na ótica dos dados?	Relação entre conhecimento sobre os dados e o sucesso da sua proteção. A gestão da informação tem influência sobre o sucesso da proteção de dados?
Padrão encontrado Gestão da informação Responsabilidade Facilita, útil	"É, mas estamos a falar do sector da saúde [...]" (P6.V2.1 – P1ULSNA#01)	"É vantajoso haver esta consciência para que os dados servem." (P6.V2.1 – P2ULSNA#02)
	"[...] reconheço que todos os processos de recolha e de tratamento de dados não estão claramente documentados e conhecidos, sabe-se qual o objetivo da recolha dos dados, mas não se conhece as limitações da sua utilização." (P6.V2.1 – P1ULSNA#01)	"[...] maioria das pessoas não tem conhecimento sobre os objetivos da recolha dos dados e as limitações na sua utilização." (P6.V2.1 – P2ULSNA#03)
	"Claro, concordo a questão. Até podem existir campos que nem sequer são utilizados, ou mesmo mal utilizados." (P6.V2.1 – P2ULSNA#02)	"Podem existir profissionais que podem deturpar a utilização de dados, e utilizar estes dados para outros fins." (P6.V2.1 – P1USF#01)
	"Sem dúvida, [...] quando se concebe uma aplicação, temos que conhecer a sua realidade de aplicação, caso contrário podemos estar sujeitos a fugas." (P6.V2.1 – P2ULSNA#03)	"[...] um conhecimento massificado dos objetivos da utilização de dados facilitava a compreensão de medidas de proteção de dados." (P6.V2.1 – P2USF#02)
	"[...] é importante, acima das questões de segurança, as pessoas olharem para estas questões com outra atenção." (P6.V2.1 – P1USF#01)	"[...] é mais fácil perceber as medidas de proteção desses dados. Quando recolho dados junto do utente, eu tenho que explicar ao utente porque estou a recolher aqueles dados." (P6.V2.1 – P3USF#06)
	"Sim muito." (P6.V2.1 – P3USF#03)	"Facilita-se depois o desenho daquilo que é a privacidade. Infelizmente, não é uma prática nossa, a documentação, justificação e enquadramento de cada processo.
	"Claro que sim, facilita." (P6.V2.1 – P3USF#04)	"[...] este é um assunto que nos preocupa, até para nos justificarmos perante instituições oficiais que nos controlam no sentido de demonstrar quais os princípios que não cumprimos." (P6.V2.1 – P1INEM#01)
	"Claro que sim [...]" (P6.V2.1 – P3USF#06)	"Sendo esta uma prática comum entre todas as organizações seria depois mais fácil desenvolver políticas de privacidade comuns e até para auditar e verificar se está ou não a ser cumprido. Até porque as instituições apresentam processos comuns de recolha de dados, o que pode ser uniformizado." (P6.V2.1 – P1INEM#01)
	"Sim e perceber quais são os seus limites." (P6.V2.1 – P1INEM#01)	"Não temos esta cultura incutida e a maior parte das pessoas não se inibe de fornecer os seus dados em qualquer formulário *online* que tenha de preencher." (P6.V2.1 – P2INEM#03)
	"Poderia ajudar, está muito dependente da cultura de cada um. Existem situações em que se recolhem dados em que a pessoa nem sequer tem a noção da legislação nem qualquer tipo de informação." (P6.V2.1 – P2INEM#03)	"[...] deveria haver uma maior informação sobre o objetivo da recolha de dados. Seria para nós mais útil, no sentido de negociarmos certas especificações do sistema." (P6.V2.1 – P2INEM#04)
	Sim. Normalmente os processos de recolha de dados não são documentados, pelo menos por nós. Limitamo-nos muitas vezes a desenhar os processos de acordo com as especificações que alguém determina." (P6.V2.1 – P2INEM#04)	"Se para as pessoas for suficientemente claro a utilização que se vai dar aos dados, facilita depois a introdução de políticas de privacidade. É muito importante saber qual é o objetivo. Qual a aplicação dos dados? Quais as consequências?" (P6.V2.1 – P2INEM#09)
	"Sim, porque quando há uma recolha de dados deve haver uma preocupação com a utilização destes dados. Estes dados servem para quê? Em várias situações me interroguei sobre o porquê de eu estar a fornecer determinados dados." (P6.V2.1 – P2INEM#09)	"Com a experiência as políticas de privacidade são mais fáceis de compreender do que numa fase inicial. É importante nesta fase explicar às pessoas o que é necessário fazer e o porquê!" (P6.V2.1 – P3INEM#05)
	"Agora nas organizações [no meio da saúde], se se pretender implementar políticas rigorosas de privacidade é exigível às pessoas que conheçam o objetivo para que se está a recolher os dados." (P6.V2.1 – P2INEM#10)	"Concordo que quanto mais se conhecer o objetivo das recolha de dados mais fácil é a compreensão da justificação das politicas de privacidade. Até porque as coisas estão interligadas. Se eu perceber o porquê da recolha de dados é mais fácil entender a razão da sua proteção." (P6.V2.1 – P3INEM#06)
	"É importante ter em conta a cultura de privacidade existente." (P6.V2.1 – P2INEM#10)	"Qualquer processo de recolha de dados, bem esclarecido, facilita a proteção daqueles dados." (P6.V2.1 – P3INEM#07)
	"[...] naquilo que é o trabalho deles as pessoais queixam-se de terem mais dados do que os necessários. Numa fase inicial as pessoas registam dados e apresentam algumas dúvidas sobre o destino daqueles dados, mas depois percebem da sua importância, da sua vantagem." (P6.V2.1 – P3INEM#05)	"Sem dúvida que a organização da informação é sem dúvida um excelente ponto de partida. Até na atribuição de responsabilidades." (P6.V2.1 – P1HFF#01)
	"Sim, as pessoas deveriam ter mais informação e estar mais informadas sobre os processos de recolha de dados. Tenho alguma dificuldade em desligar-me do meu papel, da prática clinica." (P6.V2.1 – P3INEM#06)	"Agora se houver um conhecimento geral sobre o objetivo da recolha de dados, facilita
	"Em determinadas circunstâncias poderemos estar a recolher dados que não estão relacionados ou são em demasia." (P6.V2.1 – P3INEM#07)	

	“Aquilo que é gestão da informação, pura e dura, é um facilitador para trabalhar as questões da privacidade. Posso agregar e definir políticas de utilização da informação.” (P6.V2.1 – P1HFF#01)	depois as medidas de privacidade.” (P6.V2.1 – P2HFF#02)
	“Sim, perceber-se de uma forma clara e transparente, porquê estes dados, qual o objetivo da recolha destes dados.” (P6.V2.1 – P2HFF#02)	“É prática comum dentro do hospital documentar todos os processos de recolha de dados, assim como a definição de um responsável setorial pelos processos de recolha de dados.” (P6.V2.1 – P2HFF#02)
	“Por vezes recolhemos dados a mais e depois passado algum tempo verificamos que fazem falta a determinados estudos.” (P6.V2.1 – P2HFF#02)	“E este é um aspeto importante para percebermos políticas de proteção. Os atores que constroem esta informação não têm ainda estas preocupações, de definir isto. Cá está mais uma vez a importância da maturidade, na preocupação em manter a coerência da informação.” (P6.V2.1 – P2HFF#03)
	“[…] voltamos à gestão da informação, ao pormenor, à granulidade dos dados.” (P6.V2.1 – P2HFF#03)	“A nossa preocupação é que um item de informação, só esteja num local. E se existir em vários que seja atualizável e emigrável. Temos sempre a informação mais atual. Sobre isto é depois mais fácil aplicar regras de privacidade no acesso à informação.” (P6.V2.1 – P2HFF#03)
	“No dia-a-dia a verdade é que não questionamos muito o porquê da recolha de determinados dados. Muitas vezes só depois de termos dado ou recolhidos determinados dados, é que que colocamos a questão “para que é que isto é preciso?” (P6.V2.1 – P3HFF#04)	“Concordo que havendo um conhecimento maior sobre aquilo que é o objetivo da recolha de dados, a responsabilidade sobre a recolha de dados fica depois mais fácil compreender as políticas de privacidade aplicadas. Existe uma ligação direta. Há um retorno.” (P6.V2.1 – P3HFF#04)
	“No domínio da saúde deveria haver mais informação sobre o objetivo da recolha de dados, mais informação sobre responsabilidade na recolha de dados, porque sobretudo em termos de saúde pública existe uma coisa em que nós culturalmente não somos muito pródigos, que é aquilo que entendo como fazendo parte do exercício de cidadania, e de facto nós não exercemos essa cidadania de forma útil à sociedade em si.” (P6.V2.1 – P3HFF#04)	“Nós internamente tivemos a necessidades de implementar uma política de análise e extração de dados.” (P6.V2.1 – P1SPMS#02)
	“Sim concordo. Acho que é importante que estas questões sejam mais trabalhadas nas organizações, nomeadamente ao nível da gestão da informação. Descrever e compreender os processos de recolha de dados, qual é a justificação, tem que haver um maior conhecimento destas questões.” (P6.V2.1 – P1SPMS#02)	“Facilitava depois aquilo que são políticas de privacidade e proteção de dados. Esta questão ao se tutelada e gerida por organismos diferentes, dificulta que se promova um maior conhecimento.” (P6.V2.1 – P2SPMS#03)
	“Deveria existir um maior conhecimento.” (P6.V2.1 – P2SPMS#03)	“Antes em suporte papel era muito mais fácil. Se tentarmos aplicar aqui políticas de privacidade a estes processos estas não vão ter sucesso. Pelo menos da forma como as coisas são agora.” (P6.V2.1 – P1HES#01)
	“Sim deveria haver um maior conhecimento. Nós aqui temos essa preocupação. Estamos a desenvolver políticas de utilização e cedência de dados.” (P6.V2.1 – P2SPMS#04)	“Sim se na recolha de dados nos limitarmos a recolher a informação que nos faz falta e não recolher informação a mais é óbvio que vamos ter aqui uma maior facilidade ao nível da privacidade dos dados, até porque estamos a trabalhar com menos informação.” (P6.V2.1 – P2HES#02)
	“Deveria haver uma aposta maior ao nível da gestão da informação.” (P6.V2.1 – P2SPMS#04)	“É necessário conhecer a criticidade de cada processo. E depois é mais fácil identificar onde devemos ter mais cuidados de proteção.” (P6.V2.1 – P2HES#03)
	“Sim as pessoas deveriam saber mais sobre o objetivo da recolha de dados. Os profissionais deveriam trabalhar mais a componente de gestão a informação. Olhar para os dados com outra atenção.” (P6.V2.1 – P1HES#01)	“Havendo um conhecimento sobre estes processos, mais críticos, depois é mais fácil a aplicação de medidas de proteção, de uma política de proteção.” (P6.V2.1 – P2HES#03)
	“As pessoas hoje em dia debitam a informação para dentro dos sistemas de informação sem qualquer preocupação. Existem muitos processos em que não existe um conhecimento a 100% do porquê do registo daquela informação.” (P6.V2.1 – P1HES#01)	“Se as pessoas conhecessem o porquê da recolha de dados, com algum detalhe, facilitava depois a aplicação de algumas medidas de proteção.” (P6.V2.1 – P3HES#05)
	“Deveria haver mais gestão da informação, estudar e documentar mais os processos, o tratamento de dados.” (P6.V2.1 – P2HES#02)	“Quando num episódio, em suporte papel, se pedia os episódios anteriores conseguia-se dois ou três.Com toda a disponibilidade de informação que a gente tem hoje em dia, é completamente diferente.” (P6.V2.1 – P3HES#05)
	“Existe um grande desconhecimento sobre os objetivos da recolha de dados.” (P6.V2.1 – P3HES#05)	Se existisse uma gestão da informação nas organizações, permitiria ter uma noção maior sobre os dados. Sobre os que são críticos, dados que são reservados, e dados que podem ser disponibilizados. E em função disto abordar os mecanismos de proteção. Em função do tipo de informação, eu vou ou não investir em mecanismos de proteção. A questão da organização da informação, é onde eu vou catalogar as peças da informação e vou perceber da sua criticidade, sensibilidade. Esta identificação e organização da informação, é uma tarefa que só um gabinete de segurança e privacidade pode realizar. Fala-se muito em *chief information security officer*, onde é suposto ter alguém responsável que trata destas questões da gestão da informação, que está diretamente relacionada/focada com a privacidade. Não tenho dúvidas que um profissional especializado em gestão da informação poderia facilitar todo este processo, mas que
	“Dois aspetos: (1) a informação sai para o exterior dos sistemas e perdemos o controlo e o rasto; (2) nós agora podemos ir a um repositório tirar informação que antes não existia. Nós conseguimos dar muito mais informação porque estamos cada vez mais a concentrá-la e estrutura-la “ (P1.V2.2 – P2HFF#03)	
	“Um dos pilares fundamentais desta questão da privacidade de dados é	

	precisamente a maturidade ao nível da gestão da informação" (P3.V2.1 – P2HFF#03)	evoluísse para assuntos que não têm apenas a ver com TI. (P2.V3.1 – P1HFF#01)

P6.V3.1	Necessidade de uma nomenclatura de classificação dos dados É uma ferramenta facilitadora no desenvolvimento de medidas de proteção dos dados?	Desafios ao seu desenvolvimento. Quais os principias desafios para o domínio de colaboração/interoperabilidade?
Padrão encontrado Padrão/*standard* Acesso aos dados Gestão da informação	"Seria sem dúvida." (P6.V3.1 – P1ULSNA#01)	"Mas não existe uma nomenclatura diretamente relacionada com a privacidade. Existe o senso comum, ou seja tudo o que se considera informação clinica considera-se informação sensível, obviamente terão os seus níveis de segurança." (P6.V3.1 – P1ULSNA#01)
	"Com toda a certeza." (P6.V3.1 – P2ULSNA#02)	"Tendo várias organizações a utilizar e partilhar dados é necessário que elas entendam os dados da mesma maneira, que a linguagem seja comum." (P6.V3.1 – P2ULSNA#02)
	"Sim. De certa forma existe esta classificação nas aplicações que temos, mais orientadas para níveis de acesso.	"Faz sentido, haver uma nomenclatura, de forma ser mais fácil a partilha desses dados." (P6.V3.1 – P2ULSNA#03)
	"É desejável existir uma nomenclatura partilhada por todas as organizações de saúde [...]" (P6.V3.1 – P2ULSNA#03)	"[...] permitindo por exemplo perceber quais os perigos da junção dos diferentes tipos de dados." (P6.V3.1 – P2ULSNA#03)
	"Sim é importante a existência de uma nomenclatura. Já existem diferentes níveis de acesso ao nível do utilizador, nomeadamente para médicos e profissionais de enfermagem." (P6.V3.1 – P1USF#01)	"[...] para que a proteção seja o mais homogénea possível entre instituições." (P6.V3.1 – P1USF#01)
	"É importante que exista uma partilha desta nomenclatura [...]" (P6.V3.1 – P1USF#01)	"Ao nível dos dados do processo clinico é que faz sentido esta proteção e dados através de nomenclaturas, através da classificação de dados (...). Em determinadas situações a classificação dos dados pode complicar, por exemplo o consentimento." (P6.V3.1 – P2USF#02)
	"Quem estiver a trabalhar com as nomenclaturas sabe de certeza o que é aquilo, a que se referem e para que servem. Neste momento as aplicações são todas verticais, em que o acesso aos dados é apenas controlado com base no perfil do utilizador. Um médico por exemplo, não sendo o "dono" do processo clinico, ele tem que ver toda a informação do utente." (P6.V3.1 – P2USF#02)	"Facilitava a definição de perfis de acessos. Ou seja saberíamos que perante um determinado nível do utilizador, que dados lhe podemos dar. Existem níveis de autenticação, mas depois este controlo de acesso é relegado para as aplicações. Cada aplicação tem a sua forma única de gerir o acesso à informação, ou como é que trabalhamos essa informação." (P6.V3.1 – P1INEM#01)
	"Sim facilitava, nomeadamente à equipa de IT." (P6.V3.1 – P1INEM#01)	"Esta classificação de dados para o domínio da colaboração deveria evoluir no sentido de definir os vários perfis ou camadas de dados, até onde podem ser partilhados, assim como a definição de dados que nunca podem ser partilhados." (P6.V3.1 – P1INEM#01)
	"Existe contexto para adotar ou pelo menos adaptar um *standard* neste domínio." (P6.V3.1 – P1INEM#01)	"Facilitava a interoperabilidade entre organizações ou entre aplicações, e mesmo ao nível local – existe cada vez mais a necessidade de integração das aplicações umas com as outras [...]" (P6.V3.1 – P1INEM#01)
	"Faria sentido uma nomenclatura neste aspeto. [...] Poderia passar apenas pela adaptação de um *standard* a esta necessidade." (P6.V3.1 – P2INEM#03)	"Ao nível da partilha de dados entre organizações, tem que haver um grupo, ou alguma entidade que define e que apresente um *standard*, que seja cumprido por todos de forma homogénea. Caso contrário não se consegue definir políticas iguais para tratar a mesma coisa." (P6.V3.1 – P2INEM#03)
	"Sim. Neste momento não é uma prática comum a classificação dos dados, nem a utilização de um *standard* de classificação.	"Passar para todas as organizações este tipo de nomenclatura faria com que pudessem ser mais facilmente ajustadas a medidas de segurança. É uma ideia que terá que ser mais bem assimilada por todos nós." (P6.V3.1 – P2INEM#04)
	"Não será muito fácil colocar uma nomenclatura a ser partilhada por todas as organizações e até mesmo dentro das organizações. Mas seria útil!" (P6.V3.1 – P2INEM#04)	"Sim, havendo uniformização é mais fácil a aplicação de políticas de privacidade aos dados." (P6.V3.1 – P2INEM#09)
	"Sim, se conseguíssemos ter uma nomenclatura, ficava muito facilitada a aplicação de políticas de privacidade." (P6.V3.1 – P2INEM#10)	"É necessário definir o que é importante classificar, e como classificar. Ou seja, o que é reservado, da esfera pessoal. Assim sempre que existe tratamento de dados, eles deveriam ser imediatamente classificados." (P6.V3.1 – P2INEM#09)
	"Concordo com a exigência diferenciada dos dados. Dai já termos falado em risco e criticidade dos dados, gestão da informação, análise de risco – sobre esta informação qual o grau de risco?" (P6.V3.1 – P1HFF#01)	Passávamos a ter níveis de sensibilidade, o que facilitava a generalização das políticas. Poderia ter dados que durante a fase de utilização tinha uma categoria, mas quando passava para o armazenamento, tinha outra categoria. Teria sem dúvida uma adaptação
	"No que toca à classificação de dados a ISO270001 já contempla várias sugestões quanto ao desenvolvimento de uma nomenclatura. Agora apesar da ideia, do interesse, da existência de um projeto a este nível, ainda não existe uma nomenclatura implementada." (P6.V3.1 – P1HFF#01)	
	"Sim uma nomenclatura iria facilitar a aplicação de políticas de privacidade." (P6.V3.1 – P2HFF#02)	
	"Eu julgo que sim. Esta nomenclatura existe, mas é ainda muito macro, que é capaz de não cumprir totalmente. Aquilo que muitas vezes existe depende daquilo que a prática clinica diz. Ou seja, aquilo que forem as orientações	

clinicas, porque muita da privacidade, no universo clinico, tem a ver com o que faz sentido ser consultado, por que ator e em que contexto." (P6.V3.1 – P2HFF#03)	muito mais dinâmica de políticas." (P6.V3.1 – P2INEM#10)
"O que existe hoje é muito macro – temos informação da enfermagem, informação médica, ou informação médica de psiquiatria." (P6.V3.1 – P2HFF#03)	Entre organizações, permitiria a garantia na semelhança dos processos de utilização e armazenamento de dados. Se isto for uma solução, significa que tem que haver uma partilha desta nomenclatura." (P6.V3.1 – P2INEM#10)
"Sim uma nomenclatura destas seria bastante útil." (P6.V3.1 – P1SPMS#02)	Estamos a partilhar dados, pelo que os meus dados têm que ter as mesmas medidas de proteção do outro lado." (P6.V3.1 – P2INEM#10)
"A única forma que temos e controlar o acesso aos dados é com base no perfil do profissional (role-based)." (P6.V3.1 – P1SPMS#02)	Uma nomenclatura facilitava certamente aquilo que são políticas sobre a passagem de dados entre organizações, em que era possível saber se esta informação estava sinalizada como informação critica ou não. Uma nomenclatura a este nível, generalizada nas organizações, facilitava a passagem de dados entre organizações nomeadamente através da classificação da sua criticidade, sensibilidade e segurança" (P6.V3.1 – P1HFF#01)
"Eu acho que é preciso trabalhar mais neste domínio, olharmos para os dados independentemente das aplicações, ter algo muito claro, orientações de como classificar informação com vários níveis de privacidade." (P6.V3.1 – P1SPMS#02)	"Esta nomenclatura deveria acompanhar o ciclo de vida dos dados, desde o registo até ao próprio armazenamento." (P6.V3.1 – P2HFF#02)
"Definir estas regras é sempre útil, aplicáveis a qualquer cenário de utilização de dados, assim como ter um vocabulário dentro da privacidade." (P6.V3.1 – P1SPMS#02)	"[…] esta nomenclatura deve ser partilhada. Crescer como um todo. Existem instituições com mais experiência a este nível que outras. Todas as instituições são mais reacionárias do que proactivas." (P6.V3.1 – P2HFF#02)
Se esta nomenclatura fosse um *standard* partilhado por todas as organizações, era depois mais fácil aplicar medidas de proteção. Só mesmo partindo de um *standard* internacional, uma ISO por exemplo, é que se conseguiria implementar este requisito." (P6.V3.1 – P2SPMS#03)	"Agora a transferência de dados deveria depender à partida de uma padronização dos dados deste género. Nós temos dois tipos de transferência: entre sistemas dentro da mesma entidade, e entre sistemas de entidades diferentes." (P6.V3.1 – P2HFF#03)
"Se existisse uma nomenclatura de classificação de dados, que de alguma forma fosse partilhada pelas instituições, ficava facilitado aquilo que é a relação dos conjuntos de dados com os conjuntos de profissionais e não os dados como um todo. Acho que isto é urgentíssimo.	"Agora quando os dados passam para outro sistema, externo, um *metadado* pode transportar esta nomenclatura." (P6.V3.1 – P2HFF#03)
"No fundo é criar um *standard*." (P6.V3.1 – P2SPMS#04)	"Porque de certa forma também nos permite avaliar se temos que estudar um pouco mais a forma como estamos a divulgar determinada informação." (P6.V3.1 – P1SPMS#02)
"Os dados têm de ter o mesmo significado e valor em todo o lado, caso contrário temos políticas de proteção muito díspares. E agora vamos começar, com o EpSOS a trocar dados com a europa." (P6.V3.1 – P2SPMS#04)	"Nós sabemos o quanto ela é crítica, se pode ser utilizada para outros fins, mas não temos como a classificar. Seria bastante útil uma sinalética que permitisse definir, não só o tipo de informação, mas também a questão de privacidade, se é ou não critica." (P6.V3.1 – P1SPMS#02)
"Os dados têm significados diferentes, valores e objetivos diferentes, sensibilidades diferentes." (P6.V3.1 – P1HES#01)	"Com uma categorização da informação nós poderíamos disparar um alarme quando a informação não está a ser utilizada de forma correta." (P6.V3.1 – P1SPMS#02)
"Agora uma nomenclatura para de alguma forma poder classificar os dados para depois ser mais fácil aplicar políticas de privacidade, da responsabilidade dos responsáveis pelos sistemas de informação." (P6.V3.1 – P1HES#01)	"Os mecanismos de autorização ficam facilitados." (P6.V3.1 – P2SPMS#03)
"Não fazemos gestão da informação, fazemos apenas gestão de sistemas." (P6.V3.1 – P1HES#01)	"O ideal é que o acesso aos dados não fosse apenas condicionado pelo perfil do utilizador, mas também por esta camada intermédia de classificação de dados, que permitissem mais filtros em termos de visualização." (P6.V3.1 – P2SPMS#03)
"Hoje já fazemos uma mapeamento parecido através do perfil do utilizador." (P6.V3.1 – P1HES#01)	"Quando os dados num sistema tiverem associados um determinado risco, e se depois passarem para outro sistema e tiverem o mesmo nível associado, então teremos um sistema eficiente em termos de proteção de dados." (P6.V3.1 – P2SPMS#04)
"Sim concordo que sim. Uma nomenclatura facilitava depois a aplicação de políticas de privacidade." (P6.V3.1 – P2HES#02)	"Havendo uma nomenclatura que pudesse ser partilhada, facilitava aquilo que é o propósito da partilha de dados. Eu posso decidir que determinado grupo de dados não são para partilhar." (P6.V3.1 – P1HES#01)
"Sim a adaptação de uma nomenclatura de classificação dos dados, facilitava depois a aplicação de medida de proteção destes dados. A proteção de dados seria mais focada, mais objetiva." (P6.V3.1 – P2HES#03)	"Teria como efeito prático uma garantia de acesso seguro a essa informação." (P6.V3.1 – P2HES#02)
"Esta nomenclatura tinha que ser igual para todos, tipo um *standard*. Uma norma que teria que ser respeitada por todos." (P6.V3.1 – P2HES#03)	"A nomenclatura é também importante quando partilhamos dados com outras organizações. […] Se nós tivéssemos já uma nomenclatura sabíamos já quais os níveis ou categorias de classificação dos dados, e eu sei que para um determinado nível eu tenho um conjunto de medidas." (P6.V3.1 – P2HES#03)

P6.V4.1

Relação com a proteção de dados

O que é preponderante para otimizar esta dependência?

Padrão encontrado

Uniformização tecnológica

Standard

Proteção centrada nos dados

Dependência tecnológica	Conhecimento
"É necessário alinhar a proteção de dados em todas as organizações e as medidas de acesso físico." (P6.V4.1 – P2ULSNA#02)	"[…] uma linguagem comum em proteção de dados." (P6.V4.1 – P2ULSNA#02)
"Tecnicamente começo logo a pensar nos níveis de segurança, backups, firewall e o controlo de acesso aos dados. Se tivermos uma segurança das infraestruturas e em simultâneo uma segurança da informação asseguradas, teremos com certeza o cenário ideal. Teremos assim uma resposta boa do lado da infraestrutura, e do lado dos dados, garantias que cumprimos a normas de segurança, ou seja uma situação ideal." (P6.V4.1 – P2USF#02)	"A preparação para a partilha é preponderante […]" (P6.V4.1 – P2ULSNA#03)
"Uma harmonização tecnológica pode facilitar em parte." (P6.V4.1 – P2INEM#03)	"São necessários meios humanos principalmente, a reunião das pessoas e a análise do que pretendem partilhar em concreto." (P6.V4.1 – P2ULSNA#03)
"A tecnologia é preponderante, quanto mais desenvolvimento tecnológico mais garantias para a proteção de dados." (P6.V4.1 – P2INEM#04)	"[…] um consenso sobre os dados e como os devemos começar a proteger." (P6.V4.1 – P2USF#02)
"Independentemente dos sistemas serem diferentes, esta partilha de dados está muito dependente da tecnologia, devendo existir de algum modo alguma harmonização tecnológica." (P6.V4.1 – P2INEM#09)	"Se tivermos *standards*, algo que todos consigam cumprir, melhor. Facilita sem sombra de dúvidas. Se houver um conjunto de regras que sejam comuns, *standards*, classificação de dados, facilita-se depois a privacidade como um todo." (P6.V4.1 – P2INEM#03)
"Para operacionalizar esta questão, é necessário também pensar-se na integridade tecnológica e de seguida na forma de partilha de dados." (P6.V4.1 – P2INEM#10)	"Deveria haver uma maior prática na utilização de *standards*, por exemplo ao nível da segurança, ao nível de desenvolvimento de interfaces, para garantir determinados níveis de qualidade." (P6.V4.1 – P2INEM#04)
"Ao nível da segurança as tecnologias aplicáveis são preponderantes, sendo que a interoperabilidade técnica a este nível é cada vez mais facilitada. Os próprios sistemas já trazem mecanismos de segurança implementados." (P6.V4.1 – P2HFF#02)	"[…] saber quais é que são os dados que para a saúde no seu todo, podem ser tratados e como devem ser protegidos." (P6.V4.1 – P2INEM#09)
"Nós nunca vamos conseguir otimizar esta dependência se não tivermos informação de forma estruturada." (P6.V4.1 – P2HFF#03)	"A interoperabilidade está a ajudar, mas por vezes pode não ser fácil. É necessário objetivos comuns entre todas as organizações a este nível [privacidade dos dados]." (P6.V4.1 – P2INEM#09)
"Neste momento temos muitos hospitais a organizar a sua informação de maneiras muito distintas, o que complica depois um processo de segurança, e tipificação com a semântica da proteção de dados." (P6.V4.1 – P2HFF#03)	"[…] deveria começar por sensibilizar as pessoas. É o ponto fulcral. É necessário que as pessoas tenham noção da forma com que lidam com os dados." (P6.V4.1 – P2INEM#10)
"Ou seja o 1º requisito é ter uma estrutura de dados, bem tipificada, saber-se que uma nota de alta tem que ter aquela informação, é acedível por estes atores, por exemplo. Os objetos que constituem a informação do processo clinico deveriam ser claros." (P6.V4.1 – P2HFF#03)	"Havendo a presença de um *standard* para estas questões, melhor ainda, assim como uma nomenclatura de classificação dos dados." (P6.V4.1 – P2INEM#10)
"A heterogeneidade tecnológica já não é um considerando muito forte. A partir do momento em que eu tenho informação estruturada […]" (P6.V4.1 – P2HFF#03)	"É necessário que as pessoas não contornem o risco. Tudo isto só funciona se for eficaz, controlado, otimizado de forma continua. É necessário reduzir os riscos de intrusão, de perdas de dados, ou outros riscos." (P6.V4.1 – P2INEM#10)
"A camada de segurança já é muito uniforme em termos nacionais, é já muito equivalente. As tecnologias utilizadas são muito comuns." (P6.V4.1 – P2SPMS#03)	"[…] haver um grupo que dinamize estas questões, que verifique as dificuldades que cada entidade tem, e eventualmente apresentar soluções para as ultrapassar. Muitas vezes a solução passa pela partilha [de experiências]." (P6.V4.1 – P2INEM#10)
"Existem vários mecanismos de autorização. Necessitamos de um mecanismo comum, aceite por todas as partes de autorização." (P6.V4.1 – P2SPMS#03)	"[…] é importante haver standards que de alguma forma facilitem a colaboração, haver um conjunto de padrões – padronização das melhores práticas de segurança, requisitos para um sistemas seguro, uma taxonomia." (P6.V4.1 – P2HFF#02)
"Estamos muito dependentes das tecnologias. São necessárias normas, regras que ajudem as pessoas a desenvolver esta dependência. Mesmo nos centros de saúde temos 4 ou 5 sistemas clínicos instalados, em que as coisas são feitas de maneiras diferentes." (P6.V4.1 – P2SPMS#04)	"Fazer uma proteção mais focada nos dados e não tanto nas infraestruturas." (P6.V4.1 – P2HFF#02)
"[…] tem que haver uniformidade em todas as organizações que irão colaborar. Com sistemas homogéneos tudo iria trabalhar muito melhor. Iriamos diminuir muitos riscos, tanto ao nível da segurança como ao nível das interfaces." (P6.V4.1	"No futuro nós temos que caminhar para uma privacidade focada nos dados e não apenas nas infraestruturas. Já falamos disto." (P6.V4.1 – P2HFF#03)
	"A proteção e a privacidade deveriam ter o mesmo nível de entendimento. Um *standard* a este nível ajudaria certamente." (P6.V4.1 – P2SPMS#03)
	"Podemos mover uma proteção centrada na segurança para uma proteção centrada no cidadão." (P6.V4.1 – P2SPMS#03)
	Uniformização diz respeito à utilização de *standards* que permite que todos

	– P2HES#02)	trabalhem da mesma maneira. Ao nível da segurança os *standards* são uma realidade. Com base num *standard* é depois mais fácil definir um conjunto de medidas de segurança." ((P6.V4.1 – P2HES#02))
	"Em termos de segurança de infraestruturas não estamos mal, apesar de margem de evolução, já cumprimos com os mínimos." (P6.V4.1 – P2HES#03)	"A privacidade tem que caminhar em dois sentidos: para o lado dos dados e para o lado das infraestruturas, porque se fizermos só a análise de dados um ataque à infraestrutura pode colocar em causa a privacidade daqueles dados. Neste momento a maior concentração é ao nível das infraestruturas, no patamar da segurança." (P6.V4.1 – P2HES#02)
		"É necessário um *standard* que permita a passagem de informação entre sistemas. Um *standard* que permite segurança. Se alguém apanha o ficheiro não consegue identificar a pessoa a que diz respeito." (P6.V4.1 – P2HES#03)

3. Data Display

P6	**Matriz de análise da opinião sobre P6. Dados e manipulação de dados**		
Variáveis dependentes	*Padrão encontrado*	*Suporte ao conhecimento sobre os dados* *(Que ferramentas e conhecimentos a desenvolver no domínio dos dados)*	*Desenvolvimento através da colaboração* *(itens ou questões com potencialidade de interoperabilidade)*
P6.v1. À semelhança da proteção de dados, a privacidade de dados deve ser preocupação constante durante todo o ciclo de vida dos dados em ambientes de interoperabilidade.	Conhecimento insuficiente Falta de informação Medidas específicas	O conhecimento sobre as limitações da utilização dos dados é insuficiente. As limitações não estão presentes. É necessário uma maior preparação organizacional sobre a gestão dos dados - ausência de proatividade. Aprofundar o conhecimento (atualmente insuficiente) sobre os limites na utilização dos dados e os riscos associados. Profissionais especializados para o suporte à proteção de dados. Existe um maior conhecimento das fases de criação e utilização dos dados. A transferência de dados está a apresentar grandes desafios e preocupações.	Definição de direitos e obrigações e as melhores práticas de utilização de dados. Desenvolvimento da gestão da informação. Conhecimento partilhado sobre o funcionamento dos processos de partilha de dados entre organizações. Alinhamento de medidas de proteção para situações de transferência de dados/partilha de dados. Apresentar medidas específicas para todo o ciclo de vida dos dados. Diretrizes de arquivo e armazenamento de dados.
P6.v2. A existência de procedimentos para analisar o tipo e quantidade de dados pessoais recolhidos (a sua adequação e relevância) em relação ao(s) objetivo(s) definido(s), o seu período de retenção (não mais que o necessário), assim como a transparência, clarificação e publicação destes procedimentos são essenciais à compreensão e definição de medidas de proteção da privacidade dos dados.	Gestão da informação Responsabilidade Facilita, útil	Somente com uma maior experiência e conhecimento ao nível dos dados é possível implementar políticas de privacidade que sejam facilmente compreendidas. No meio da saúde, se se pretende implementar políticas rigorosas de privacidade é exigível às pessoas que conheçam o objetivo para que se está a recolher os dados. É importante, útil, vantajoso, existir um maior conhecimento e informação sobre os dados, o objetivo da sua recolha. A organização da informação é um ponto de partida. É necessário documentar todos os processos. Ajustar a proteção de dados à criticidade de cada processo. A maturidade ao nível da gestão da informação é fundamental.	Desenvolvimento de princípios orientadores para as organizações com processos comuns de recolha de dados. Desenvolvimento das melhores práticas de documentação do objetivo do processo de recolha de dados, dos detalhes dos dados, das limitações de utilização, das consequências da má utilização dos dados. Criar condições para a demonstração do compromisso para com a proteção de dados e para a realização de auditorias. Desenvolvimento da gestão da informação no suporte ao conhecimento sobre os dados, os processos, e no desenvolvimento conjunto de políticas de proteção. Preparar profissionais em gestão da informação.
P6.v3. A classificação, dinâmica (durante todo o seu ciclo de vida), dos dados é essencial à definição dos níveis de proteção e privacidade pretendidos, assim como os domínios onde pode circular, isto é dentro da organização e entre organizações.	Padrão/*standard* Acesso aos dados Gestão da informação	Faz sentido um padrão, uma nomenclatura de classificação dos dados – facilita o desenvolvimento e aplicação de políticas de privacidade. Neste momento o acesso aos dados é apenas controlado com base no perfil de utilizador. Facilita o conhecimento da criticidade, sensibilidade, disponibilidade e risco associado aos dados. Nomenclatura de classificação para todo o ciclo de vida.	Desenvolvimento ou adaptação de um *standard* para a classificação dos dados. Uniformização das medidas de proteção para os processos de partilha de dados. Alinhamento das políticas de partilha de dados. Garantir que a classificação de dados não se altera quando estes são partilhados entre sistemas.
P6.v4. A privacidade dos dados depende diretamente (1) do âmbito, (2) das tecnologias aplicadas e (3) dos *standards* usados da/na proteção de dados, implementados localmente e em ambientes de interoperabilidade. Quanto mais granular melhor. Quanto mais interoperáveis melhor.	Uniformização tecnológica *Standard* Proteção centrada nos dados	Uma harmonização tecnológica, integridade tecnológica podem facilitar a proteção de dados. É necessário regularizar a evolução tenológica. A estruturação dos dados e a organização da informação, são um fator de maior importância. São necessários padrões/standards no suporte à classificação dos dados, das melhores práticas de segurança e do funcionamento da interoperabilidade.	Definição de objetivos comuns para a privacidade dos dados. Definição nos padrões de suporte ao programa de proteção de dados. Desenvolvimento de estruturas de dados (Ex: conceito de processo clinico eletrónico). Meios humanos especializados em proteção de dados, capazes de fomentar uma proteção mais centrada nos dados. É necessário que as pessoas não contornem o risco.