Análise dos dados – P8. Confiança e gestão da confiança

1. Dados das entrevistas

Variável dependente – Participante

P8.V1.1

P8.V1.1 – P1ULSNA#01	É necessário gerir este fator que se chama confiança. É fundamental promover para este tipo de questões uma política global que envolva sem dúvida um grupo de profissionais-chave de diversos locais. Irá sem dúvida fomentar a confiança institucional. É importante identificar os níveis de confiança em relação à colaboração das restantes organizações no domínio da privacidade dos dados? Sim e caminhar de forma tentar colocar de forma homogénea esses níveis de confiança em todas as instituições. A experiência aumenta a confiança na interoperabilidade organizacional. Tem que haver níveis de acesso aos dados. Os dados devem ser disponibilizados com níveis de acesso rigorosos. Existem dados sensíveis, menos sensíveis e públicos. A confiança tem que existir. A informação médica tem que circular entre os diversos médicos. Se a informação médica não circular entre todos os médicos, vai acontecer uma coisa muito simples, tenho dificuldade em atuar cada vez mais em relação ao meu colega, se tiver um doente que fez um enfarte, e me desaparecer da minha lista de utentes durante cinco anos, eu não tenho informação quando ele regressar a mim. Acontece, é vulgar. A informação tem que circular livremente entre os diversos grupos profissionais. A ULSNA corresponde a um domínio de confiança no que troca à troca de informação. Tenho um sistema ALERT P1 que permite que para cada consulta, fazer a patologia do doente, sintomas, mas depois não tenho informação de retorno. E, se eu quiser saber a informação da ULSNA também não consigo. Fico completamente cego quando envio o doente para uma consulta externa do hospital. Nem recebo informação por escrito.
P8.V1.1 – P4ULSNA#06	Admito que possa estar a mudar a atitude de desconfiança, mas se muda não é por intervenção ou consciência das organizações, mas sim porque ela é de certa maneira imposta. Mesmo em relação à própria tutela nós temos alguma dificuldade em disponibilizar dados. É sempre muito complicado disponibilizar dados quando podem acarretar riscos de responsabilização se não for acautelada a sua proteção. Por isso é fundamental a definição de uma estratégia, que trace um caminho comum, que permita identificar processos comuns. A criação de um grupo de trabalho para estas questões apenas por iniciativa das instituições é difícil de acontecer, seriam sempre situações pontuais. As pessoas não vão conseguir perceber os benefícios que a criação do grupo de trabalho poderia trazer para a instituição. Questões desta natureza, nomeadamente no que toca à proteção de dados, ou existe um desenvolvimento concertado, muito bem planeado, ou então ele não vai nascer pela iniciativa de duas instituições e gradualmente influenciar outras instituições. É o exemplo da instalação dos sistemas ALERT nas urgências, o qual poderia ter sido um processo concertado e não foi, acabando por ser muito prejudicial para as organizações.
P8.V1.1 – P1USF#01	O sistema informático, principalmente aquele em que os médicos trabalham todos os dias, foi desenvolvido com a sua ajuda e colaboração. Houve aqui uma interação entre os técnicos de informática e os médicos. Existe hoje em dia uma maior facilidade de

	colaboração entre equipas.
P8.V1.1 – P4USF#05	Tem que existir a iniciativa de alguém, com reuniões, colóquios, em que a pessoa partilhe conhecimento com outros. As pessoas têm que ser instruídas com este conhecimento.
P8.V1.1 – P1INEM#01	Seria vantajoso para no global tudo funciona-se melhor. Tudo depende muito da confiança entre as organizações. Até sou da opinião, que dentro do ministério da saúde, deveria funcionar como uma cultura, um grupo de trabalho transversal a todos os organismos para depois ser mais fácil de implementar [medidas]. Cada vez mais as equipas de IT estão reduzidas aos mínimos e não temos tempo para nos dedicarmos a estes assuntos. Em último caso, eu diria, um dos parentes pobres do IT é a segurança. Muitos de nós damos muita atenção à laboração, e pouco à segurança [...]. Ou seja, o principal foco de uma equipa IT nunca é a segurança. Ou temos equipas dedicadas à segurança, ou a segurança está sempre em segundo plano. Para esta questão da proteção de dados era desejável uma colaboração entre as organizações, nomeadamente na partilha de conhecimento, na adoção de soluções conjuntas. [...] Se o topo das organizações estiverem sensibilizados para estas questões será mais fácil. Partir de um plano estratégico para o desenvolvimento da proteção de dados ao nível do próprio ministério. Hoje em dia, e cada vez mais, trabalhamos de acordo com o que somos obrigado a cumprir.
P8.V1.1 – P4INEM#08	A questão é que para nós conseguirmos determinados objetivos para a partilha da informação, e que sabemos que são determinantes para obter resultados na prestação de cuidados na área da saúde em concreto, leva a que nós avancemos com integrações de processos com a noção dos riscos, mas que se assumem para obter um determinado resultado. Na realidade depois também temos que ver o reverso da medalha – nós não avançamos com um determinado processo porque não está garantida a proteção de dados. Quando um processo clinico está em formato digital, na rede, toda a gente está preocupada com a proteção dos dados, mas quando ele circula num hospital na mão de uma pessoa ninguém se preocupa. Acho que hoje existem níveis muito elementares de proteção ou de garantia do acesso seguro aos dados, que não respondem aos requisitos que permitam a garantia total, mas se nós não avançarmos por ai, tentando obter o ótimo, então não temos nada. E o que se perde pode ser muito. Este processo tem que se fazer com a introdução de ferramentas, de requisitos, à medida que vamos desenvolvendo os sistemas de informação, que permitam dar resposta a isto (proteção de dados). Os sistemas de informação desenvolvidos interorganizações apresentam uma confiança intrínseca. Confia-se à partida. Habitualmente discute-te os riscos e o nível de segurança. Tomam-se medidas muitas vezes porque se percebe que existem falhas de segurança. Para corrigir. Mas é com base na confiança em todos, e que todos estamos a utilizar a informação da melhor forma para os resultados que se pretende.
P8.V1.1 – P1HFF#01	A gestão da confiança nasce de cima. É cá em cima (ARS, SPMS) que tem que ser dito o que fazer às organizações - que atualmente funcionam muito isoladas, muito para si. Quem está cá em cima é quem consegue ver a floresta e não apenas uma árvore. Dou um exemplo de falta de interoperabilidade, que durante décadas inibiu e não permitiu o desenvolvimento da verdadeira telemedicina em Portugal - a falta de criação de protocolos de entendimento entre as várias organizações, centros de saúde e hospitais em várias regiões, que deveriam ser induzidos pelo ministério, fez com que a telemedicina não evoluísse como o desejado. As coisas evoluíram apenas por iniciativas individuais. Alguns exemplos através dos projetos de cidades digitais.
P8.V1.1 – P4HFF#05	Existe uma confiança intrínseca entre as organizações em situações de partilha de dados. Atualmente o core da partilha de dados é a PDS. As questões de segurança não se colocam porque existe uma confiança que suporta todo o processo. Nem nós nem eles têm os citérios para a segurança e para a privacidade totalmente definidos, no âmbito da partilha de informação.

	Agora as organizações deveriam ter modelos para gerir a confiança com outras organizações, dada a avalanche contínua de partilha de dados. Dai que a creditação das organizações ajude a esta confiança. Neste momento nós não questionamos a transferência de dados através da PDS. Numa situação de partilha de serviços, em que a sua eficiência depende de todas as partes, a confiança é importante, nomeadamente na área técnica.
P8.V1.1 – P1SPMS#02	Como estou mais ligado à parte técnica tenho alguma dificuldade em responder a questões de interoperabilidade organizacional.
P8.V1.1 – P1HES#01	É fundamental desenvolver-se a interoperabilidade organizacional entre organizações da mesma área, neste caso na saúde. Nos antes tínhamos algumas coisas com a ULSNA, tínhamos uma relação muito próxima, em que desenvolvemos algumas soluções de interligação. Neste momento já temos alguma interoperabilidade com Beja, nomeadamente na área da anatomia patológica. Temos uma ligação para transferência de informação com o hospital de Badajoz, autorizada pela CNPD, que demorou dois anos a autorizar. Mas são coisas muito residuais, muito pontuais. Mais uma vez, se os Estado fosse regulador e certificados, acho que potenciava este tipo de iniciativas. A privacidade e a proteção de dados é sempre um tema a abordar sempre que há colaboração com outra instituição. A partir do momento em que a informação clinica deixa de estar arquivada em papel e passa a circular livremente nas redes, seja dentro da saúde, na Internet, a privacidade tem que ser sempre posta no 1º nível de discussão. Temos que desenvolver esta interoperabilidade dentro do ministério da saúde. Nós não partilhamos quase nada. Cada um trabalha por si. Seria saudável a existência de grupos que permitissem desenvolver medidas de proteção de dados mais eficientes. A confiança entre organizações é a partida importante para iniciativas de colaboração. Caso contrário não se desenvolvem pontes de colaboração. Sempre que do outro lado está um sistema de informação não confiável, não seguro, dificilmente se partilha dados. Daí a nossa não adesão à PDS.

P8.V2.1

P8.V2.1 – P1ULSNA#01	Bastante. A nível dos utilizadores nem tanto. Independentemente de onde vêm os dados, estes pretendem é visualizar os dados num determinado local. Agora do ponto de vista técnico a influência é muito grande. O caminho passa por criar sistemas mais homogéneos. Contudo é necessário pensar nos sistemas legados, em que a sua mudança seria muito dispendiosa e complexa, onde é necessário definir em políticas de interoperabilidade que tenham em atenção a privacidade. Cá está privacidade diferente de segurança.
P8.V2.1 – P4ULSNA#06	Pode. Apesar de anteriormente ter afirmado que esta geração é mais tecnológica, que coabita naturalmente com as tecnologias e sistemas de informação e muito facilmente entende e assimila estes conceitos, nós ainda estamos numa fase de transição, sendo que no futuro a utilização de múltiplos sistemas será totalmente transparente.
P8.V2.1 – P1USF#01	Não é o caso da ARS Norte. Para o caso de cuidados de saúde primários, existe apenas um sistema – SAME – utilizado em todas as unidades de cuidados de saúde primários, não existindo aquela dispersão aplicacional. Há outras aplicações, nomeadamente do rastreio do cancro, pedido de consulta hospitalar … Acho que as pessoas não pensam muito na confiança em relação aos sistemas. Queixam-se muito na complexidade de utilizar várias aplicações, mas nunca se dirigiram a mim com esta preocupação. Até porque existe um grau de confiança naquilo que nós fazemos, apesar de haver muitas pessoas que criticam o facto de utilizarem múltiplas aplicações. A confiança é essencialmente gerida através da segurança. Nós nunca demos razões às pessoas para pensarem de outra forma. Quando se implementou o SAME, as principais críticas estavam relacionadas com o objetivo de controlo, que se destinava a que o ministério controla-se o que os profissionais de saúde faziam, mas depois as pessoas vieram a constatar que de facto não era este o

	objetivo. A múltipla autenticação é uma das críticas mais frequentes. Está neste momento a trabalhar-se numa nova ferramenta de prescrição – PEM - em que um dos principais objetivos é aumentar o nível de segurança ao nível do acesso dos profissionais. Um profissional no SAME pode prescrever, não sendo controlado se o profissional está ou não no ativo, ao passo que a PEM já valida o profissional junto de uma lista fornecida pela Ordem dos Médicos
P8.V2.1 – P4USF#05	Gosto mais de funcionar só com um sistema. Tem que haver uma base comum a todos os sistemas, para que depois seja mais fácil a sua utilização. Uma maior cultura de privacidade pode levar as pessoas a colocar mais questões sobre os dados destes sistemas. Questionarem possíveis fugas de informação. Reservarem mais os dados.
P8.V2.1 – P1INEM#01	Numa primeira análise diria que sim. Depende do tipo de dados que estamos a partilhar. Porque é diferente se estamos a partilhar dados como a morada, ou algo de identificação, que não é sensível, ou quando começamos a partilhar dados mais sensíveis, mais pessoais. Havendo algo que certifique esta utilização seria de todo vantajoso. No fundo haver uma instituição que controlo a partilha de dados e que ao mesmo tempo tenha processo de fiscalização sobre os dados. Saber a qualquer momento o que está a ser feito com os dados e como estão a ser partilhados. O cidadão normal comum, não tem esta capacidade de rastreabilidade dos dados, sobre o que é que estão a fazer com os nossos dados. É cada vez mais uma realidade.
P8.V2.1 – P4INEM#08	Por incrível que pareça não. A cultura da privacidade está a mudar no cidadão. Existe nos profissionais de saúde uma aceitação da partilha de dados, uma vez que é para seu bem. Nunca questionaram este poder. Sempre se assumiu que se podia transferir dados de saúde de uma forma transparente, sem grande preocupação. A cultura do cidadão é que está a mudar no sentido que querer garantia da sua privacidade. Temos que perceber que vamos que ter que ir atrás daquilo que é a mudança da cultura do cidadão face a esta matéria. As pessoas começam a perceber se acontecem quebra de privacidade nas redes sociais, podem também acontecer em outros sistemas.
P8.V2.1 – P1HFF#01	No geral não. A desconfiança nestas situações até vai sendo atenuada. Isto porque os sistemas de informação dependem cada vez de aplicações sobre bases de dados. Isto no caso do IT ter efetivamente politica definidas e procedimentos muito baseados em *single sign-on*, e uma boa gestão da identidade digital. Ou seja, o próprio colaborador/profissional tem que ter a consciência do seu perfil. É desejável que esta gestão da identidade possa evoluir para uma federação de confiança. É o que estão a tentar fazer na SPMS. São os casos da identidade dos profissionais de saúde, com o RNU. A consolidação numa única plataforma de toda a informação sobre os funcionários através do RHD, para mim é um caminho para garantir que eles sabem, quem é que trabalha nos hospitais, e que tem de uma forma federativa a possibilidade de fazer um controlo a nível nacional sobre os profissionais. Cada hospital vai ser obrigado a "beber" informação de identificação numa base de dados nacional. É o melhor caminho para mitigar problemas locais de gestão da identidade digital.
P8.V2.1 – P4HFF#05	Os dados quando saem [são partilhados] têm de ser naturalmente estruturados. Esse é o âmbito da PDS, os dados. O âmbito do acesso aos dados não deve ser a qualquer profissional de saúde, é um risco. Temos e conseguir a rastreabilidade do profissional, de forma a saber a que dados acedeu, que dados alterou. Esta estruturação de dados pode garantir a privacidade e proteção de dados. Se houver um alinhamento dos requisitos de privacidade entre as organizações que colaboram na PDS, vai no fundo aumentar a confiança das pessoas em relação a aquilo que estão a partilhar. Eu não sei é se as pessoas já estão despertas para esta necessidade. Por exemplo o Portal do Utente tem inscrições espontâneas. Quantas pessoas foram ler com atenção as regras de privacidade e de acesso à informação? Quantas questões foram enviadas a quem está a gerir aquela plataforma? Na partilha de dados com outras organizações podemos perder o rasto de quem está a consultar os dados. Nós, atualmente apenas

	conseguimos saber quem nos está a consultar os dados que temos armazenados. A partir do momento em que os dados são transferidos para outro sistema, para serem reutilizados, perco a noção de onde estão estes dados, e isto é uma preocupação, apesar de esta reutilização ser um sinonimo de melhoria. A interoperabilidade é um meio de reutilização de dados.
P8.V2.1 – P1SPMS#02	Sim de certa forma influencia. Em relação ao sistema clinico instalado a nível nacional no setor público pelo ministério, os profissionais estão bem ambientados, sabem qual é a informação partilhada. Mas se estiverem a operar com sistemas de outros fornecedores, menos conhecidos pelos profissionais, as pessoas têm desconfiança. Identificam informação que falta, questionam a forma de partilha de informação. Estamos a trabalhar nesta área, ao tentar incorporar uma vista única sobre os dados, e não estar a mostrar diretamente o processo clinico daquele lado. Por vezes os profissionais têm a noção que estão a dar mais do lado da sua instituição e não estão a receber do outro. Há uma maior transparência.
P8.V2.1 – P1HES#01	Falamos de utilizadores de uma forma geral? Sinceramente, sou da opinião que não condiciona. Continuo a achar, enquanto utente, aquilo que condiciona tem a ver com o facto de eu não saber, o quê, onde, e como. Eu não sei o que é partilhado sobre a minha informação clinica, não sei onde é que ela está a ser guardada, e eu não sei que políticas de segurança e de responsabilização existem. A única coisa que eu sei é que provavelmente alguém neste país já tem toda a minha informação que está na PDS. Isto, eu sei. E isto assusta-me, pois estamos a falar de informação perigosíssima [...]. E isto sim é que condiciona os utilizadores. Depois não há transparência em relação ao que a PDS faz. Ou seja, eu não acho que a utilização de múltiplos sistemas seja condicionante, desde que os SPMS certificassem e regulassem a utilização dos dados e dos sistemas. Ou seja, se a SPMS em vez de fazer *software*, regulasse a aplicação de software, definisse os requisitos, certificasse, seria mais positivo.

P8.V3.1

P8.V3.1 – P1ULSNA#01	Esta análise não tem sido feita. As pessoas ainda não pensão nestas questões. Só o vão fazer com o desenvolvimento de um cultura e sensibilidade quanto à privacidade. As pessoas só vão pensar nesta questão quando algo de muito expositivo suceder. Comparo muitas vezes esta questão da privacidade com a utilização das redes sociais. A maior parte destas pessoas expõe factos da sua vida nas redes sociais e não tem a mínima noção de privacidade. Esta informação pode inclusive ser usada contra eles mesmo profissionalmente. No desenvolvimento de novas soluções a análise do seu impacto sobre a privacidade é relegada para um 2º plano, o que não deveria acontecer. O nosso desenvolvimento apenas engloba dados tratados internamente, em que não vai haver qualquer partilha, com qualquer outro departamento ou outra instituição. E falamos na maioria das vezes de dados não sensíveis, mas identificáveis.
P8.V3.1 – P4ULSNA#06	Sim tem um feito direto na confiança das pessoas. É necessário salvaguardar a privacidade. As pessoas têm receio de ser facilmente escrutinadas. Num ambiente de desconfiança tenho de certeza alguma dificuldade em exercer a minha atividade.
P8.V3.1 – P3ULSNA#04	Penso as atuais aplicações não são avaliadas em relação ao impacto sobre a privacidade, e não vejo necessidade desta aplicação.
P8.V3.1 – P1USF#01	Acho que esta análise seria muito útil. Sinceramente, não sei se esta análise é feita. Concordo que deve existir uma grande preocupação a este nível, é uma questão que me preocupa. Existe a este nível um organismo muito importante e que dita muitas regras e condiciona muitas vezes aquilo que se pretende fazer, que é a CNPD. Não há nada que seja implementado sem a sua aprovação. Por exemplo existiu um projeto que consistia num cartão que armazenava informação de saúde do utente, medicamentos a prescrever, etc. que não foi implementado porque a CNPD não autorizou.

P8.V3.1 – P3USF#03	Sem dúvida deveria investir-se mais numa análise prévia. Mesmo alguns equipamentos médicos deveriam ser mais uniformizados quanto a esta questão. A este nível, mais a nível hospitalar, cada hospital comprava o que queria, o que foi muito mau. Penso que a administração central deveria efetuar este controlo. A transmissão aos profissionais de saúde de que determinada solução foi testada quando à privacidade funcionava como um selo de confiança. Por exemplo algumas aplicações são-nos apresentadas, e de imediato nos pedem para "registar". Não nos é indicado como proceder em relação a estas questões. Estes assuntos não são precavidos.
P8.V3.1 – P3USF#04	Esta análise prévia era o ideal. Teoricamente era o ideal. Na prática como o fazer, não sei. As pessoas vão ter mais confiança, ao saberem das políticas de privacidade e do impacto que poderão ter no futuro, com base num estudo. Deveria haver uma maior preocupação em relação ao que se recolhe e qual o impacto que pode ter sobre o utente, nomeadamente ao nível da imagiologia, quer para o lado do médico quer do utente.
P8.V3.1 – P3USF#06	É importante. Só que quando se implementa alguma destas tecnologias, compreendo que seja difícil faze-lo antes. Agora que é importante, é. Uma análise anterior de impacto sobre a privacidade estimulava por exemplo a confiança dos profissionais de saúde nestas tecnologias. Só que nós no SNS não estamos muito habituados a isto! Normalmente os programas surgem de um dia para o outro e nós desenrascamo-nos. É esta a nossa prática. Vamos aprendendo com a utilização.
P8.V3.1 – P4USF#05	Apesar de não saber como se fará esta análise, acho que sim, seria importante esta análise. Sim, penso que a confiança dos profissionais aumentaria (…). Deveria ser uma prática comum.
P8.V3.1 – P1INEM#01	Deve-se avaliar o impacto sobre a privacidade. Isto não quer dizer que se faça. Não é ainda uma prática. Deveria ser um princípio! Normalmente trabalha-se ao contrário – primeiro adquire-se ou desenvolve-se e só depois é que se analisa. Incutir um princípio destas passaria pela cultura, sendo que desenvolver cultura é difícil. Era necessário sensibilizar as pessoas responsáveis. Uma análise de risco bem-feita, que permitisse também cobrir a privacidade dos dados, se calhar alertava as pessoas para a análise do impacto sobre a privacidade. Na prática primeiro pensa-se em determinada solução e só depois é que se pensa em licenciar, em proteção de dados, etc. Quando no levantamento inicial deveria ser analisada esta questão. […] no nosso caso existem medidas especificas, planos de contingência para o hardware ao nível dos equipamentos que andam nas ambulâncias. Por exemplo não guardamos o histórico do paciente no computador local, os dados estão sempre remotamente centralizados. Tentamos limitar o risco na utilização dos equipamentos que possa expor dados. Se perdemos um equipamento, a perda é só do *hardware* e não de dados.
P8.V3.1 – P3INEM#05	Sim, penso que era importante esta análise prévia. Nunca desviando do conceito e do objetivo inicial da tecnologia, do que se está a tentar melhorar, do processo, mas não se deve descorar a questão da privacidade. Vai de encontro ao que eu disse no início - estamos a trabalhar com dados em que as pessoas se veem obrigadas a fornecer. Ainda não é uma prática comum este tipo de análise, talvez porque as pessoas que estão envolvidas nos processos de melhoria não apresentam formação neste sentido e não sabem o que é que está em causa. Pensam que privacidade é "fechar tudo aqui" e não passar nada a ninguém. A privacidade não significa manter tudo em segredo, mas sim manter seguro e utilizar de forma correta.
P8.V3.1 – P3INEM#06	Há sim. Deve haver sempre uma análise. Acho que o princípio deve ser sempre o balanço entre o risco e o benefício. Tem de haver sempre esta análise (…).
P8.V3.1 – P3INEM#07	Acho que sim deveria ser feita uma análise de impacto sobre a privacidade de qualquer solução tecnológica. Da mesma maneira que falamos do impacto "ambiental" deveríamos falar dom impacto sobre a privacidade antes de qualquer solução entrar em produção. Provavelmente poderiam aumentar o custo das ferramentas, mas de certeza que aumentaria a segurança e a confiança em relação aos

	fins. Lembro-me de algumas soluções que nós utilizamos internamente que deveriam ser mais "fechadas" do que são atualmente. Quando foram desenvolvidas não consideraram a proteção do individuo, mas apenas armazenar dados.
P8.V3.1 – P4INEM#08	Sim, deveria haver uma matriz de risco. Cada vez que se trate de dados, que possam ter a ver com a privacidade das pessoas (…) acho que estas situações devem ser abordadas com uma matriz de risco, e essa matriz de risco deve determinar o comprimento de determinados requisitos dai para a frente. Nós neste momento fazemos isso numa ou outra matéria – que é perante uma reclamação, antes de dar num processo de inquérito, ou num processo disciplinar, vai para uma matriz de risco, e em função desta é tomada a decisão de qual o procedimento a tomar. Este modelo pode ser utilizado para tomar decisões relativamente aos procedimentos a ter ao nível de investimento ou de certificação. Esta ainda não é uma prática ao nível dos sistemas de informação.
P8.V3.1 – P1HFF#01	Eu diria que não é apenas vantajoso – é essencial. Aqui não falamos de tecnologias, mas sim de um modelo processual. O epSOS é um bom exemplo a este nível. Porque privacidade tem muito a ver com proteção. Privacidade e proteção são de alguma forma tudo risco. A ISO 27005 ajuda na identificação e prova de que existe risco. O epSOS baseia-se nesta norma. É um modelo que vai ao limite da pessoa – o que é que ela faz, etc. Inclui a identidade digital, a segurança física, a segurança lógica, os comportamentos, as politicas. Agora só vamos conseguir ter uma análise de risco, e conseguir fazer alguma coisa, se esta tiver origem ao nível da gestão. Caso contrário não se consegue fazer nada. Se não houver risco, para é que eu estou preocupado com a privacidade? É com base no risco que nós conseguimos sustentar na opinião pública, nos parceiros, o que é que está em causa. Não é contudo fácil fazer esta análise. Isto deve ser encarado como um processo. Posso usar uma ferramenta de *risk management*, que me assegura todas as cláusulas e tópicos e subtópicos que tenho que endereçar para garantir a privacidade da informação. Atualmente a análise de risco é mais focada nas questões de segurança. Na disponibilidade dos sistemas, logo mais tecnológica. É ainda muito IT management.
P8.V3.1 – P3HFF#04	Deveríamos ter linhas orientadoras, um determinado padrão. Um padrão que poderia ser um tronco comum nacional, visto que tecnologias deste tipo têm impacto em várias organizações, e depois dentro de cada região verificar os impactos positivos ou não. Sendo isto realizado criava uma maior confiança e uma maior qualidade dos dados transportados, e uma verdadeira rede colaborativa. Porque toda a gente falaria exatamente do mesmo no momento.
P8.V3.1 – P4HFF#05	É importante que seja feita esta avaliação [análise de impacto sobre a privacidade] com certeza. Ainda não é uma prática comum. Também não tem sido uma preocupação dos utilizadores em conhecer este tipo de análise. Agora, sendo uma preocupação que surja dos utilizadores, esta análise pode ajudar a que estes confiem nas soluções em funcionamento.
P8.V3.1 – P1SPMS#02	Sim sem dúvida. Deveria ser uma prática mais comum. Normalmente os sistemas de informação são desenhados com base em objetivos, sem a análise do risco em relação à privacidade. Não temos noção do risco. Desenhemos um sistema de informação, ele vai para o terreno, e depois é que se levantam as questões. Acho que isto deveria ser algo a ter em conta logo na fase de análise. Deveríamos perceber logo à partida qual o impacto sobre a privacidade, os efeitos negativos sobre a privacidade.
P8.V3.1 – P1HES#01	A primeira coisa que eu acho que devia ser feita, e uma vez que a PDS está criada, e de uma forma aberta, deveria ser uma análise de risco. Faz todo o sentido. Nós não temos ainda a noção do risco, uma vez que a nossa análise do risco é ainda muito limitada à segurança. Apesar de ainda não ser feita de uma forma estruturada. Resulta apenas das conversas entre técnicos. Ainda não é um processo documentado. Agora uma análise do risco na área dos dados seria fundamental, e estamos a pensar fazer iniciar este processo.

	A proposta do nosso auditor interno, realizada este ano ao nível dos sistemas de informação, levantou uma série de questões, que habitualmente se identificam. E um dos nossos objetivos é perceber em relação aos dados, se nós estamos a fazer as coisas de forma correta, se os dados estão efetivamente salvaguardados, se as políticas de segurança que estamos a implementar são as mais corretas. Não é uma análise de robustez. Uma análise de risco pode ser um ponto de partida, perceber onde estão riscos associados. Nós muitas vezes não temos esta noção. O mesmo deveria acontecer com a PDS. Deveriam ter analisado os sistemas onde residem os dados e quais os riscos associados. Instituições como a nossa que utilizam grandes quantidades de dados têm obrigatoriamente de trabalhar com base numa análise do risco. Risco ao nível da informação e risco ao nível das infraestruturas. [...]
P8.V3.1 – P3HES#05	Eu acho que os riscos dependem das patologias. Acho que devíamos pensar no risco de uma nova plataforma atempadamente, para o doente. Nem que não seja apenas para validar a aplicação informática. É fundamental, quanto mais difícil for o acesso à aplicação melhor. Agora também é verdade que se for a alguns sítios, tem uma série de perfis abertos para consultar o que quiser. Não é só o risco das aplicações, mas também dos utilizadores. [...] Não é prático encerrar a sessão de trabalho, nem a autenticação através da impressão digital. Muitas vezes as pessoas utilizam *passwords* uns dos outros. Os sistemas têm nomes de pessoas que já nem trabalham cá, estão reformados! Os informáticos têm que ter uma atitude pró-ativa em relação a isto e saber quais os utilizadores a serem eliminados do sistema. De repente até os administrativos acedem aos dados clínicos. Durante muito tempo alguns utilizadores tiveram que se adaptar às tecnologias e serem capazes da sua utilização. Hoje já estamos noutro patamar. A utilização das tecnologias já não é um problema. Tornamo-nos dependentes dos computadores, e em todo o lado tem que haver um computador. O problema agora são os dados, o acesso a todos os dados. Temos a ideia que meia-dúzia de pessoas chegava para gerir tudo isto, e não chega.
P8.V3.1 – P4HES#06	A pessoas dão sempre o exemplo do HIV, como um grupo de risco, que é necessário proteger. Mas se for uma situação de interrupção voluntária de gravidez não tem o mesmo risco. Uma pessoa que tem um cancro que vai morrer daqui por 3 meses, a pessoa tem a obrigação que os outros saibam que ele vai morrer. Existe um conjunto de dados que é plausível que eles sejam cedidos, disponibilizados com muita facilidade, mas há outros que não podem em situação nenhuma ser partilhados. Neste caso falamos de dados objetivos do doente, que são do direito do doente. Outra coisa completamente diferente é o trabalho intelectual feito pelo técnico, que é registado a cada episódio. Dados de risco extremo, deveriam ficar de imediato isolados e não serem acedidos por mais ninguém.

2. *Data Reduction*

P8.V1	Confiança como pilar fundamental A confiança é um fator determinante ao desenvolvimento de iniciativas de partilha de dados.	Influência sobre a partilha de dados Como pode ser gerida? Quais os aspetos a considerar?
Padrão encontrado Essencial à partilha de dados Importante	"É necessário gerir este fator que se chama confiança. É fundamental promover para este tipo de questões uma política global que envolva sem dúvida um grupo de profissionais-chave de diversos locais." (P8.V1.1 – P1ULSNA#01)	"A experiência aumenta a confiança na interoperabilidade organizacional." (P8.V1.1 – P1ULSNA#01)
	"Admito que possa estar a mudar a atitude de desconfiança, mas se muda não é por intervenção ou consciência das organizações, mas sim porque ela é de certa maneira imposta." (P8.V1.1 – P4ULSNA#06)	"É sempre muito complicado disponibilizar dados quando podem acarretar riscos de responsabilização se não for acautelada a sua proteção. Por isso é fundamental a definição de uma estratégia, que trace um caminho comum, que permita identificar processos comuns." (P8.V1.1 – P4ULSNA#06)
	"Existe hoje em dia uma maior facilidade de colaboração entre equipas." (P8.V1.1 – P1USF#01)	"Questões desta natureza, nomeadamente no que toca à proteção de dados, ou existe um desenvolvimento concertado, muito bem planeado, ou então ele não vai nascer pela iniciativa de duas instituições e gradualmente influenciar outras instituições." (P8.V1.1 – P4ULSNA#06)
	"Tudo depende muito da confiança entre as organizações." (P8.V1.1 – P1INEM#01)	"Numa situação de partilha de serviços, em que a sua eficiência depende de todas as partes, a confiança é importante, nomeadamente na área técnica." (P8.V1.1 – P4ULSNA#06)
	"Os sistemas de informação desenvolvidos interorganizações apresentam uma confiança intrínseca. Confia-se à partida. Habitualmente discute-te os riscos e o nível de segurança. Tomam-se medidas muitas vezes porque se percebe que existem falhas de segurança. Para corrigir. Mas é com base na confiança em todos, e que todos estamos a utilizar a informação da melhor forma para os resultados que se pretende." (P8.V1.1 – P4INEM#08)	"Tem que existir a iniciativa de alguém, com reuniões, colóquios, em que a pessoa partilhe conhecimento com outros. As pessoas têm que ser instruídas com este conhecimento." (P8.V1.1 – P4USF#05)
	"A gestão da confiança nasce de cima. É cá em cima (ARS, SPMS) que tem que ser dito o que fazer às organizações - que atualmente funcionam muito isoladas, muito para si. Quem está cá em cima é quem consegue ver a floresta e não apenas uma árvore." (P8.V1.1 – P1HFF#01)	"Para esta questão da proteção de dados era desejável uma colaboração entre as organizações, nomeadamente na partilha de conhecimento, na adoção de soluções conjuntas. [...] Se o topo das organizações estiverem sensibilizados para estas questões será mais fácil." (P8.V1.1 – P1INEM#01)
	"Existe uma confiança intrínseca entre as organizações em situações de partilha de dados. As questões de segurança não se colocam porque existe uma confiança que suporta todo o processo. Nem nós nem eles têm os citérios para a segurança e para a privacidade totalmente definidos, no âmbito da partilha de informação." (P8.V1.1 – P4HFF#05)	A questão é que para nós conseguirmos determinados objetivos para a partilha da informação, e que sabemos que são determinantes para obter resultados na prestação de cuidados na área da saúde em concreto, leva a que nós avancemos com integrações de processos com a noção dos riscos, mas que se assumem para obter um determinado resultado." (P8.V1.1 – P4INEM#08)
	"Numa situação de partilha de serviços, em que a sua eficiência depende de todas as partes, a confiança é importante, nomeadamente na área técnica." (P8.V1.1 – P4HFF#05)	Acho que hoje existem níveis muito elementares de proteção ou de garantia do acesso seguro aos dados, que não respondem aos requisitos que permitam a garantia total, mas se nós não avançarmos por ai, tentando obter o ótimo, então não temos nada. E o que se perde pode ser muito." (P8.V1.1 – P4INEM#08)
	"A confiança entre organizações é a partida importante para iniciativas de colaboração. Caso contrário não se desenvolvem pontes de colaboração." (P8.V1.1 – P1HES#01)	Este processo tem que se fazer com a introdução de ferramentas, de requisitos, à medida que vamos desenvolvendo os sistemas de informação, que permitam dar resposta a isto (proteção de dados)." (P8.V1.1 – P4INEM#08)
		Dou um exemplo de falta de interoperabilidade, que durante décadas inibiu e não permitiu o desenvolvimento da verdadeira telemedicina em Portugal - a falta de criação de protocolos de entendimento entre as várias organizações, centros de saúde e hospitais em várias regiões, que deveriam ser induzidos pelo ministério, fez com que a telemedicina não evoluísse como o desejado. As coisas evoluíram apenas por iniciativas individuais. Alguns exemplos através dos projetos de cidades digitais." (P8.V1.1 – P1HFF#01)
		"Agora as organizações deveriam ter modelos para gerir a confiança com outras organizações, dada a avalanche contínua de partilha de dados. Dai que a creditação das organizações ajude a esta confiança." (P8.V1.1 – P4HFF#05)
		"Sempre que do outro lado está um sistema de informação não confiável, não seguro, dificilmente se partilha dados. Daí a nossa não adesão à PDS." (P8.V1.1 – P1HES#01)

P8.V2	Confiança e interoperabilidade Partilhar serviços e informação pode gerar desconfiança entre os intervenientes?	Qual a implicação sobre a privacidade dos dados Quais os desafios à privacidade dos dados nestes contextos?
Padrão encontrado Influencia Controlo dos dados	"Bastante. A nível dos utilizadores nem tanto. Agora do ponto de vista técnico a influência é muito grande. O caminho passa por criar sistemas mais homogéneos." (P8.V2.1 – P1ULSNA#01)	"A nível dos utilizadores nem tanto. Independentemente de onde vêm os dados, estes pretendem é visualizar os dados num determinado local." (P8.V2.1 – P1ULSNA#01)
	"A interoperabilidade é um meio de reutilização de dados." (P8.V2.1 – P4HFF#05)	"Contudo é necessário pensar nos sistemas legados, em que a sua mudança seria muito dispendiosa e complexa, onde é necessário definir em políticas de interoperabilidade que tenham em atenção a privacidade. Cá está privacidade diferente de segurança." (P8.V2.1 – P1ULSNA#01)
	"Se houver um alinhamento dos requisitos de privacidade entre as organizações que colaboram na PDS, vai no fundo aumentar a confiança das pessoas em relação a aquilo que estão a partilhar. Eu não sei é se as pessoas já estão despertas para esta necessidade." (P8.V2.1 – P4HFF#05)	"Na partilha de dados com outras organizações podemos perder o rasto de quem está a consultar os dados. Nós, atualmente apenas conseguimos saber quem nos está a consultar os dados que temos armazenados." (P8.V2.1 – P4HFF#05)
	"Acho que as pessoas não pensam muito na confiança em relação aos sistemas. Queixam-se muito na complexidade de utilizar várias aplicações, mas nunca se dirigiram a mim com esta preocupação. Até porque existe um grau de confiança naquilo que nós fazemos, apesar de haver muitas pessoas que criticam o facto de utilizarem múltiplas aplicações. A confiança é essencialmente gerida através da segurança. Nós nunca demos razões às pessoas para pensarem de outra forma." (P8.V2.1 – P1USF#01)	"A partir do momento em que os dados são transferidos para outro sistema, para serem reutilizados, perco a noção de onde estão estes dados, e isto é uma preocupação, apesar de esta reutilização ser um sinonimo de melhoria." (P8.V2.1 – P4HFF#05)
	"Numa primeira análise diria que sim. Depende do tipo de dados que estamos a partilhar." (P8.V2.1 – P1INEM#01)	"Tem que haver uma base comum a todos os sistemas, para que depois seja mais fácil a sua utilização. Uma maior cultura de privacidade pode levar as pessoas a colocar mais questões sobre os dados destes sistemas. Questionarem possíveis fugas de informação. Reservarem mais os dados." (P8.V2.1 – P4USF#05)
	Por incrível que pareça não. A cultura da privacidade está a mudar no cidadão. Existe nos profissionais de saúde uma aceitação da partilha de dados, uma vez que é para seu bem. Nunca questionaram este poder." (P8.V2.1 – P4INEM#08)	"No fundo haver uma instituição que controle a partilha de dados e que ao mesmo tempo tenha processo de fiscalização sobre os dados. Saber a qualquer momento o que está a ser feito com os dados e como estão a ser partilhados." (P8.V2.1 – P1INEM#01)
	Sempre se assumiu que se podia transferir dados de saúde de uma forma transparente, sem grande preocupação." (P8.V2.1 – P4INEM#08)	"As pessoas começam a perceber se acontecem quebra de privacidade nas redes sociais, podem também acontecer em outros sistemas." (P8.V2.1 – P4INEM#08)
	No geral não. A desconfiança nestas situações até vai sendo atenuada. Isto porque os sistemas de informação dependem cada vez de aplicações sobre bases de dados. Isto no caso do IT ter efetivamente politica definidas e procedimentos muito baseados em single sign-on, e uma boa gestão da identidade digital. Ou seja, o próprio colaborador/profissional tem que ter a consciência do seu perfil." (P8.V2.1 – P1HFF#01)	"[…] pois estamos a falar de informação perigosíssima […]. E isto sim é que condiciona os utilizadores. Depois não há transparência em relação ao que a PDS faz." (P8.V2.1 – P1HES#01)
	"Pode. Apesar de anteriormente ter afirmado que esta geração é mais tecnológica, que coabita naturalmente com as tecnologias e sistemas de informação e muito facilmente entende e assimila estes conceitos, nós ainda estamos numa fase de transição, sendo que no futuro a utilização de múltiplos sistemas será totalmente transparente." (P8.V2.1 – P4ULSNA#06)	
	"Sim de certa forma influencia. Em relação ao sistema clinico instalado a nível nacional no setor público pelo ministério, os profissionais estão bem ambientados, sabem qual é a informação partilhada. Mas se estiverem a operar com sistemas de outros fornecedores, menos conhecidos pelos profissionais, as pessoas têm desconfiança. Identificam informação que falta, questionam a forma de partilha de informação." (P8.V2.1 – P1SPMS#02)	
	"[…] eu não acho que a utilização de múltiplos sistemas seja condicionante, desde que os SPMS certificassem e regulassem a utilização dos dados e dos sistemas." (P8.V2.1 – P1HES#01)	

P8.V3	Análise atempada dos riscos É uma prática necessária, e que deve ser regulamentada?	Influência sobre confiança dos profissionais Este conhecimento tem influencia numa maior confiança na utilização dos sistemas?
Padrão encontrado Análise prévia Principio	"Esta análise não tem sido feita. As pessoas ainda não pensão nestas questões. Só o vão fazer com o desenvolvimento de uma cultura e sensibilidade quanto à privacidade. As pessoas só vão pensar nesta questão quando algo de muito expositivo suceder." (P8.V3.1 – P1ULSNA#01)	"No desenvolvimento de novas soluções a análise do seu impacto sobre a privacidade é relegada para um 2º plano, o que não deveria acontecer. O nosso desenvolvimento apenas engloba dados tratados internamente, em que não vai haver qualquer partilha, com qualquer outro departamento ou outra instituição. E falamos na maioria das vezes de dados não sensíveis, mas identificáveis." (P8.V3.1 – P1ULSNA#01)
	"É importante que seja feita esta avaliação [análise de impacto sobre a privacidade] com certeza. Ainda não é uma prática comum." (P8.V3.1 – P4HFF#05)	"Também não tem sido uma preocupação dos utilizadores em conhecer este tipo de análise. Agora, sendo uma preocupação que surja dos utilizadores, esta análise pode ajudar a que estes confiem nas soluções em funcionamento." (P8.V3.1 – P4HFF#05)
	"Acho que esta análise seria muito útil." (P8.V3.1 – P1USF#01)	"Existe a este nível um organismo muito importante e que dita muitas regras e condiciona muitas vezes aquilo que se pretende fazer, que é a CNPD." (P8.V3.1 – P1USF#01)
	"Sem dúvida deveria investir-se mais numa análise prévia. Mesmo alguns equipamentos médicos deveriam ser mais uniformizados quanto a esta questão." (P8.V3.1 – P3USF#03)	"A transmissão aos profissionais de saúde de que determinada solução foi testada quando à privacidade funcionava como um selo de confiança. Por exemplo algumas aplicações são-nos apresentadas, e de imediato nos pedem para "registar". Não nos é indicado como proceder em relação a estas questões. Estes assuntos não são precavidos." (P8.V3.1 – P3USF#03)
	"Esta análise prévia era o ideal. Teoricamente era o ideal." (P8.V3.1 – P3USF#04)	"As pessoas vão ter mais confiança, ao saberem das políticas de privacidade e do impacto que poderão ter no futuro, com base num estudo. Deveria haver uma maior preocupação em relação ao que se recolhe e qual o impacto que pode ter sobre o utente, nomeadamente ao nível da imagiologia, quer para o lado do médico quer do utente." (P8.V3.1 – P3USF#04)
	"É importante. Só que quando se implementa alguma destas tecnologias, compreendo que seja difícil faze-lo antes. Agora que é importante, é." (P8.V3.1 – P3USF#06)	"Uma análise anterior de impacto sobre a privacidade estimulava por exemplo a confiança dos profissionais de saúde nestas tecnologias. Só que nós no SNS não estamos muito habituados a isto! Normalmente os programas surgem de um dia para o outro e nós desenrascamo-nos. É esta a nossa prática. Vamos aprendendo com a utilização." (P8.V3.1 – P3USF#06)
	Apesar de não saber como se fará esta análise, acho que sim, seria importante esta análise." (P8.V3.1 – P4USF#05)	"Sim, penso que a confiança dos profissionais aumentaria (…). Deveria ser uma prática comum." (P8.V3.1 – P4USF#05)
	Deve-se avaliar o impacto sobre a privacidade. Isto não quer dizer que se faça. Não é ainda uma prática. Deveria ser um princípio! Normalmente trabalha-se ao contrário – primeiro adquire-se ou desenvolve-se e só depois é que se analisa.	"Uma análise de risco bem-feita, que permitisse também cobrir a privacidade dos dados, se calhar alertava as pessoas para a análise do impacto sobre a privacidade." (P8.V3.1 – P1INEM#01)
	"Na prática primeiro pensa-se em determinada solução e só depois é que se pensa em licenciar, em proteção de dados, etc." (P8.V3.1 – P1INEM#01)	"Quando no levantamento inicial deveria ser analisada esta questão. […] no nosso caso existem medidas especificas, planos de contingência para o hardware ao nível dos equipamentos que andam nas ambulâncias." (P8.V3.1 – P1INEM#01)
	"Sim, penso que era importante esta análise prévia. Nunca desviando do conceito e do objetivo inicial da tecnologia, do que se está a tentar melhorar, do processo, mas não se deve descorar a questão da privacidade." (P8.V3.1 – P3INEM#05)	"Ainda não é uma prática comum este tipo de análise, talvez porque as pessoas que estão envolvidas nos processos de melhoria não apresentam formação neste sentido e não sabem o que é que está em causa. Pensam que privacidade é "fechar tudo aqui" e não passar nada a ninguém. A privacidade não significa manter tudo em segredo, mas sim manter seguro e utilizar de forma correta." (P8.V3.1 – P3INEM#05)
	"Há sim. Deve haver sempre uma análise. Acho que o princípio deve ser sempre o balanço entre o risco e o benefício. Tem de haver sempre esta análise (…)." (P8.V3.1 – P3INEM#06)	"[…] de certeza que aumentaria a segurança e a confiança em relação aos fins." (P8.V3.1 – P3INEM#07)
	Acho que sim deveria ser feita uma análise de impacto sobre a privacidade de qualquer solução tecnológica. Da mesma maneira que falamos do impacto "ambiental" deveríamos falar do impacto sobre a privacidade antes de qualquer solução entrar em produção." (P8.V3.1 – P3INEM#07)	"Este modelo pode ser utilizado para tomar decisões relativamente aos procedimentos a ter ao nível de investimento ou de certificação. Esta ainda não é uma prática ao nível dos sistemas de informação." (P8.V3.1 – P4INEM#08)
	Lembro-me de algumas soluções que nós utilizamos internamente que deveriam ser mais "fechadas" do que são atualmente. Quando foram desenvolvidas não consideraram a proteção do individuo, mas apenas armazenar dados." (P8.V3.1 – P3INEM#07)	
	"Sim, deveria haver uma matriz de risco. Cada vez que se trate de dados, que possam ter a ver com a privacidade das pessoas (…) acho que estas situações devem ser abordadas com uma matriz de risco, e essa matriz de risco deve determinar o comprimento de determinados requisitos dai para a frente." (P8.V3.1 – P4INEM#08)	

	“Eu diria que não é apenas vantajoso – é essencial. Aqui não falamos de tecnologias, mas sim de um modelo processual.” (P8.V3.1 – P1HFF#01)	“Porque privacidade tem muito a ver com proteção. Privacidade e proteção são de alguma forma tudo risco. A ISO 27005 ajuda na identificação e prova de que existe risco. O epSOS baseia-se nesta norma. É um modelo que vai ao limite da pessoa – o que é que ela faz, etc. Inclui a identidade digital, a segurança física, a segurança lógica, os comportamentos, as politicas.” (P8.V3.1 – P1HFF#01)
	“Agora só vamos conseguir ter uma análise de risco, e conseguir fazer alguma coisa, se esta tiver origem ao nível da gestão. Caso contrário não se consegue fazer nada.” (P8.V3.1 – P1HFF#01)	“É com base no risco que nós conseguimos sustentar na opinião pública, nos parceiros, o que é que está em causa. Não é contudo fácil fazer esta análise. Isto deve ser encarado como um processo.” (P8.V3.1 – P1HFF#01)
	“Atualmente a análise de risco é mais focada nas questões de segurança. Na disponibilidade dos sistemas, logo mais tecnológica. É ainda muito IT management.” (P8.V3.1 – P1HFF#01)	“Sendo isto realizado criava uma maior confiança e uma maior qualidade dos dados transportados, e uma verdadeira rede colaborativa. Porque toda a gente falaria exatamente do mesmo no momento.” (P8.V3.1 – P3HFF#04)
	“Deveríamos ter linhas orientadoras, um determinado padrão. Um padrão que poderia ser um tronco comum nacional, visto que tecnologias deste tipo têm impacto em várias organizações, e depois dentro de cada região verificar os impactos positivos ou não.” (P8.V3.1 – P3HFF#04)	“Sim tem um feito direto na confiança das pessoas. É necessário salvaguardar a privacidade. As pessoas têm receio de ser facilmente escrutinadas. Num ambiente de desconfiança tenho de certeza alguma dificuldade em exercer a minha atividade.” (P8.V3.1 – P4ULSNA#06)
	“Sim sem dúvida. Deveria ser uma prática mais comum. “Normalmente os sistemas de informação são desenhados com base em objetivos, sem a análise do risco em relação à privacidade. Não temos noção do risco. Desenhemos um sistema de informação, ele vai para o terreno, e depois é que se levantam as questões. Acho que isto deveria ser algo a ter em conta logo na fase de análise.” (P8.V3.1 – P1SPMS#02)	“Deveríamos perceber logo à partida qual o impacto sobre a privacidade, os efeitos negativos sobre a privacidade.” (P8.V3.1 – P1SPMS#02)
	“Faz todo o sentido. Nós não temos ainda a noção do risco, uma vez que a nossa análise do risco é ainda muito limitada à segurança. Apesar de ainda não ser feita de uma forma estruturada. Resulta apenas das conversas entre técnicos. Ainda não é um processo documentado.” (P8.V3.1 – P1HES#01)	“E um dos nossos objetivos é perceber em relação aos dados, se nós estamos a fazer as coisas de forma correta, se os dados estão efetivamente salvaguardados, se as políticas de segurança que estamos a implementar são as mais corretas.” (P8.V3.1 – P1HES#01)
	“Eu acho que os riscos dependem das patologias. Acho que devíamos pensar no risco de uma nova plataforma atempadamente, para o doente.” (P8.V3.1 – P3HES#05)	“Instituições como a nossa que utilizam grandes quantidades de dados têm obrigatoriamente de trabalhar com base numa análise do risco. Risco ao nível da informação e risco ao nível das infraestruturas. [...]” (P8.V3.1 – P1HES#01)
		“A utilização das tecnologias já não é um problema. Tornamo-nos dependentes dos computadores, e em todo o lado tem que haver um computador. O problema agora são os dados, o acesso a todos os dados.” (P8.V3.1 – P3HES#05)
		“Existe um conjunto de dados que é plausível que eles sejam cedidos, disponibilizados com muita facilidade, mas há outros que não podem em situação nenhuma ser partilhados. Dados de risco extremo, deveriam ficar de imediato isolados e não serem acedidos por mais ninguém.” (P8.V3.1 – P4HES#06)

3. Data Display

P8	**Matriz de análise da opinião sobre P8. Confiança e gestão da confiança**		
Variáveis dependentes	*Padrão encontrado*	*Confiança no suporte à interoperabilidade* *(Importância da confiança no funcionamento de um ambiente de partilha de dados)*	*Confiança e privacidade* *(Influência do fator confiança sobre o sucesso da privacidade dos dados)*
P8.v1. A confiança constitui um dos pilares fundamentais aos processos de colaboração entre as organizações num ambiente de interoperabilidade.	Essencial à partilha de dados	É necessário gerir a confiança. A experiência aumenta a confiança na interoperabilidade organizacional.	É sempre muito complicado disponibilizar dados quando podem acarretar riscos de responsabilização se não for acautelada a sua proteção. É necessária uma colaboração das organizações na adoção de soluções conjuntas.
	Importante	Existe hoje uma maior facilidade de colaboração entre organizações.	
		Os SI interorganizações apresentam uma confiança intrínseca. Tomam-se medidas porque se percebe que existem falhas de segurança.	Existe a noção que é necessário correr riscos na implementação de processos de integração no sentido de atingir objetivos para a partilha de dados.
		A confiança é importante, tecnicamente, numa situação de partilha de serviços, em que a sua eficiência depende de todas as partes.	Dificilmente se partilham dados sempre que do outro lado está um sistema de informação não confiável.
		A confiança entre organizações é importante para iniciativas de colaboração. São um pilar das pontes de colaboração.	É necessário um desenvolvimento concertado, por forma a influenciar todas as organizações.
P8.v2. O contexto de interoperabilidade influencia a atitude e a confiança de uma organização em relação às restantes, com implicação sobre a privacidade dos dados partilhados.	Influência	Do ponto de vista técnico a influência é muito grande. O caminho passa por criar sistemas mais homogéneos.	Na partilha de dados com outras organizações podemos perder o rasto de quem está a consultar os dados.
	Controlo dos dados	A interoperabilidade é um meio de reutilização de dados.	A partir do momento em que os dados são transferidos para outro sistema, para serem reutilizados, perco a noção de onde estão estes dados, e isto é uma preocupação, apesar de esta reutilização ser um sinónimo de melhoria.
		Se houver um alinhamento dos requisitos de privacidade entre as organizações, vai no fundo aumentar a confiança das pessoas em relação àquilo que estão a partilhar.	
		A confiança é essencialmente gerida através da segurança.	Tem que haver uma base comum a todos os sistemas, para que depois seja mais fácil a sua utilização.
		Depende do tipo de dados que estamos a partilhar.	
		Existe nos profissionais de saúde uma aceitação da partilha de dados, uma vez que é para seu bem.	As pessoas começam a perceber que se acontecem quebras de privacidade nas redes sociais, podem também acontecer em outros sistemas.
		São necessárias políticas bem definidas e procedimentos muito baseados numa boa gestão da identidade digital.	Depois não há transparência em relação ao que a PDS faz.
P8.v3. A utilização de tecnologias inerentemente invasivas da privacidade, tecnologias novas que apresentam ameaças e que provocam demasiado interesse público, representam um risco à confiança sobre o sistema.	Análise prévia	Deveria investir-se mais numa análise prévia. Avaliar o impacto sobre a privacidade deveria ser um princípio.	Sim, deveria haver uma matriz de risco.
	Princípio	Na prática primeiro pensa-se em determinada solução e só depois é que se pensa em licenciar, em proteção de dados. Os SI são desenhados com base em objetivos, sem a análise do risco em relação à privacidade.	A transmissão aos profissionais de saúde de que determinada solução foi testada quando à privacidade funcionava como um selo de confiança.
		Este modelo pode ser utilizado para tomar decisões relativamente aos procedimentos a ter ao nível de investimento ou de certificação.	A privacidade não significa manter tudo em segredo, mas sim manter seguro e utilizar de forma correta.
		Deveríamos ter linhas orientadoras, um determinado padrão.	Privacidade e proteção são de alguma forma tudo risco. A ISO 27005 ajuda na identificação e prova de que existe risco. O epSOS baseia-se nesta norma.
		Não temos ainda a noção do risco, uma vez que a nossa análise do risco é ainda muito limitada à segurança.	Deveríamos perceber logo à partida qual o impacto sobre a privacidade, os efeitos negativos sobre a privacidade.
		É com base no risco que nós conseguimos sustentar na opinião pública, nos parceiros, o que é que está em causa.	A utilização das tecnologias já não é um problema. Tornamo-nos dependentes dos computadores, e em todo o lado tem que haver um computador. O problema agora são os dados, o acesso a todos os dados.
		Criava uma maior confiança e uma maior qualidade dos dados transportados, e uma verdadeira rede colaborativa.	