Análise dos dados - P3. Segurança e infraestruturas

1. Dados das entrevistas

Variável dependente – Participante

P3.V1.1

P3.V1.1 – P1ULSNA#01	As maiores preocupações vêm sempre da segurança e não da privacidade. Ou seja a maior preocupação é que não se venha a prejudicar a origem dos dados. Ou seja nós disponibilizamos, nós queremos disponibilizar, mas de uma forma segura. Esta preocupação começa a abranger a camada de proteção de dados, também derivado às imposições legais.
P3.V1.1 – P2ULSNA#02	A unidade local de saúde é constituída pelo hospital de Portalegre e o hospital de Elvas, sendo que existe apenas um serviço de informática de apoio, uma equipa de informática. Dentro do ministério onde nós trabalhamos, o ministério da saúde, a estrutura é mais ou menos similar em termos de rede. A estrutura base nasceu em 1995/96 com a RIS (Rede de Informação da Saúde), assente em circuitos de acesso básico, circuitos digitais, que dependiam da necessidade de cada hospital. Hoje em dia a estrutura é mais ou menos similar, sendo que a ULSNA apresenta algumas coisas diferentes do país. Mas basicamente assenta numa rede de comunicação própria da saúde alugada a um operador, [...] , onde existe um endereçamento base da própria RIS e onde cada hospital tem o seu endereçamento privado, de escolha e configuração interna. Existe uma *firewall* responsável pelo controlo de acessos exteriores, assim como o controlo com outras instituições no exterior em que nós tenhamos alguma interação, em que são configuradas regras para estas instituições. As grandes diretrizes em questões de segurança vêm do mistério da saúde. A PDS é um exemplo, em que são feitas consultas diretas às nossas bases de dados, neste caso o SONHO (Sistema Integrado de Informação Hospitalar), sistema de gestão hospitalar administrativo, que existe na grande maioria dos hospitais nacionais, e ao SINUS (sistema de Informação para as Unidades de Saúde), vocacionado para os centros de saúde. Com o arranque da PDS, o ministério da saúde tem um acesso direto às nossas bases de dados, em que eles próprios criam os utilizadores necessários, sendo que a única interação que existe da nossa parte em termos de proteção é garantir que o acesso a uma determinada porta de uma máquina de uma base de dados está garantido. Ou seja o nosso papel é um pouco limitado, sendo que não controlamos os dados que são retirados. O acesso é direto por parte do exterior. Assumimos que a RIS é uma rede de confiança, contudo temos uma maior preocupação nos nossos dados, sendo que não temos preocupação em relação aos dados que os utilizadores do ministério da saúde retiram.
P3.V1.1 – P2ULSNA#03	Neste caso e no contexto da saúde, em que o principal visado é sempre o utente, existe sempre uma preocupação, quanto existe interoperabilidade de dados entre os diversos sistemas ou instituições, é sempre a privacidade dos dados, como é óbvio. Embora dentro da privacidade dos dados, me pareça que não existe muita sensibilidade para esta questão, que é uma questão muito pertinente e importante. As questões de segurança são obviamente também uma questão importante.
P3.V1.1 – P1USF#01	Só se consegue aceder a dados de saúde se o posto de trabalho estiver dentro da rede da saúde. Não é possível aos profissionais de saúde aceder a partir de casa às aplicações informáticas. O funcionamento em rede funciona assim num ambiente mais ou menos controlado. Em relação às preocupações de estar tudo em rede, pensando como utente do que como técnico, os dados são a maior preocupação. A segurança é uma das maiores preocupações, os profissionais de saúde apresentam muito esta preocupação. Por outro lado a disponibilidade dos sistemas é também uma forte preocupação. Numa rede com muitas organizações, com milhares de utilizadores, a segurança é sem dúvida uma das preocupações mais prioritárias.

P3.V1.1 – P2USF#02	Neste caso, quando queremos colocar uma unidade em rede ou um serviço em rede? São várias as questões a serem analisadas. Primeiro, quais os serviços que vamos fornecer? Que tipo de serviços vai ser fornecido? A quem vamos fornecer? Quem vai aceder? Vão ou não ter publicação de dados? Onde é que vão e não vão estar os dados? Quais as zonas que acedem aos dados? É um trabalho que começa a ser desenhado previamente. No nosso caso, e do seu conhecimento prévio, nós funcionamos com suporte da RIS (Rede Informática da Saúde) e isso por si só já nos dá algumas garantias. Depois dentro da RIS é necessário saber que tipos de serviços é que prestamos. Se são serviços apenas prestados para a RIS, ou se são serviços que vamos prestar para a RIS e para fora da RIS. E isto leva-nos a questões de segurança diferentes, porque os acessos são diferentes, a disponibilidade/colocação dos dados é feita de maneira diferente. Que tipos de dados vamos disponibilizar? São dados acedidos de fora? Vão ter *backend*? Quem vai aceder? No nosso caso tudo isto é controlado. Não conseguimos trabalhar se não for desta forma.
P3.V1.1 – P1INEM#01	Eu penso que a rastreabilidade dos dados será a preocupação maior. Serve para tranquilizar o utilizador – nós partilhamos os seus dados mas sabemos onde estão, quem foram as pessoas que acederam aos dados. Rastreabilidade de dados e também de utilizadores. São em simultâneo preocupações de segurança e preocupações de protecção de dados, dada a sua relação. A protecção de dados está muito associada à segurança. Apesar de podermos cumprir com todos os requisitos de protecção de dados mas depois a segurança falhar nitidamente. A segurança é um primeiro patamar de preocupações.
P3.V1.1 – P2INEM#03	Primeiro a segurança e a privacidade de dados. O INEM trabalha com dados sensíveis, dados que têm que respeitar regras de confidencialidade em relação a pessoas, doentes, e há que ter a garantia de que há uma estrutura preparada e uma protecção adequada destes dados. Confidencialidade, segurança, logicamente ligada à confidencialidade, são as maiores preocupações.
P3.V1.1 – P2INEM#04	Numa perspectiva geral, a maior preocupação é não haver uma dependência excessiva na tecnologia, tendo em conta que ela pode sempre a qualquer momento, e por razões diversas, não estar disponível. E isto é um objectivo que muitas vezes nós julgamos não ser atingível, ou pelo menos não ser uma prioridade. Obriga a repensar a disponibilidade dos sistemas, e não só. Mesmo em soluções de alta disponibilidade, estamos sempre a pensar que as tecnologias funcionam e muitas vezes não pensamos que pode haver situações que impeçam o seu funcionamento. Numa perspectiva do senso comum a segurança é uma das questões logo pensada. Não temos métodos escritos que nos levem a abordar esta questão numa forma muito rigorosa, mas digamos que pelo senso comum faz com que tenhamos alguma preocupação com as tecnologias e soluções de segurança.
P3.V1.1 – P2INEM#09	É a segurança. Quer em termos da utilização dos dados, quer dos próprios dados em si, neste caso através backups. Depois de 2003 começou a haver uma grande preocupação com a segurança das infra-estruturas de dados, com a instalação de datacenters protegidos. Existe hoje em dia uma maior preocupação com a segurança, que não havia aqui há uns anos. Hoje em dia o acesso aos datacenters, exige que a pessoa seja acompanhada por um dos técnicos, é necessário registar o acesso. Se a preocupação inicial foram as infra-estruturas, gradualmente começa a haver uma maior preocupação em relação á segurança da informação.
P3.V1.1 – P2INEM#10	As que são ou as que deveriam ser? As maiores preocupações neste momento estão relacionadas com a forma de implementar as soluções. Arranjar soluções que permitem que funcionem. No nosso caso em particular nem sempre é fácil, pois temos recursos muito dispersos. Aquelas que deveriam ser as maiores preocupações, e que eu quero acreditar que iram ser a curso prazo será mesmo a segurança da informação que circula. Estamos a falar no nosso caso de termos meios dispersos por todo o país, sobre ligações telefónicas basicamente, em permanência a comunicar com os servidores e a enviar informação. Depois temos que pensar em termos da segurança dos próprios equipamentos, onde o furto é uma das maiores preocupações. A confidencialidade dos dados que reside nos equipamentos

	é importante.
P3.V1.1 – P1HFF#01	Um dos principias desafios é precisamente o que temos vindo a falar – os protocolos de entendimento, a parte da interoperabilidade. Saber o que cada um faz já a ACSS faz! Mas principalmente quando se está à espera que uma organização que não está dotada de um conjunto de recursos, porque a que está ao lado tem esses recursos, a questão da interoperabilidade é crucial. E este é o principal problema – as fontes de entendimento, do ponto de vista de processos, de informação, dos sistemas de informação, que se forem diferentes obriga a criar plataforma de integração tecnológicas próprias para eu passar dados, por exemplo de imagiologia.
P3.V1.1 – P2HFF#02	O que acontece normalmente é um conjunto de "mal-entendidos". As instituições não estão habituadas a trabalhar em rede. Alguns conceitos não são compreendidos por todas as partes da mesma forma. Estes conceitos têm de ser alinhados. Nomeadamente a nível de processos. O hospital aqui faz um processo de uma determinada maneira, mas outro hospital faz o mesmo processo de uma maneira completamente diferente. Por exemplo temos um projeto de tele-radiologia com outro hospital, [...] e temos tido imenso problemas relacionados com os sistemas de informação, para interoperar com os dois sistemas. Os processos de utilização dos sistemas são diferentes, não houve formação inicial. Os principais problemas estão relacionados com a interoperabilidade não técnica. A interoperabilidade técnica, essa foi como que imediata. É muitas vezes difícil passar informação. Num hospital, que funciona 24/7, às vezes é muito complicado a informação fluir para toda a gente. Inicialmente as questões de segurança não são uma prioridade. Interessa antes de mais por os protocolos a funcionar. Fazer com que haja passagem de informação entre sistemas. Posteriormente e gradualmente as questões da segurança começam a ser colocadas e implementadas.
P3.V1.1 – P2HFF#03	Eu interpreto aqui várias temáticas ou várias áreas. Uma tem a ver, e em primeiro lugar, alguns conceitos na área clinica de interpretação da informação clinica e do que é a informação clinica, e quem é que tem acesso à informação clinica. Existem vários projectos nacionais que depois esbarram em diferentes interpretações de como é que a informação deve ser tratada e consultada. [...] Alguns projectos nacionais esbarram com aquilo que é a cultura de trabalho de alguns hospitais. Teoricamente deveria haver um alinhamento entre as direcções clinicas e ser claro quem tem o papel de quê. Ao nível da PDS a mesma coisa, quando se tenta interpretar o papel de técnicos de saúde ou dos farmacêuticos. Existe neste momento uma grande discussão [em relação à PDS], e neste hospital posso-lhe dizer que a questão de facto da privacidade – quem regista e quem consulta os dados – faz com que alguns clínicos se retraiam muito, por não se sentirem muito confortáveis no entendimento que fazem desta questão.
P3.V1.1 – P1SPMS#02	A acessibilidade da informação que é disponibilizada. Às vezes as instituições estão mais preocupadas em obter a informação do outro lado e nem tanto disponibilizar informação. A cessibilidade neste momento é crítica. No caso da RIS, o no que toca à proteção e segurança das redes há muitas falhas no acesso à informação em determinadas regiões do país, nas quais se está a trabalhar.
P3.V1.1 – P2SPMS#03	Conhecer quem está a falar com quem. Qual o nível de segurança a que isto está a acontecer. A RIS, rede privada do ministério da saúde, melhora o processo de segurança. Temos pouco parceiros Internet, que vêm do mundo externo. Ainda assim internamente carecem de regras que permitam criar comunicações com uma maior fiabilidade. O facto de não haver regulamentação, nem nenhum organismo com esse tipo de responsabilidade, e que obrigue, significa cada entidade com autonomia financeira instala e desenvolve os sistemas na forma como entende. Não conseguem ainda ser as normas a estabelecer as regras para a interoperabilidade ao nível da segurança.
P3.V1.1 – P2SPMS#04	Em termos de preocupação é mesmo a partilha dos dados, em termo de segurança, de quem acede, e mesmo também, falando mais da parte para a qual estou mais sensibilizada, que é o volume de informação. Muitas vezes é muito fácil dizer que temos que fazer partilha de dados, de ter interoperabilidade, de disponibilizar os dados, mas depois não podem ser disponibilizados todos os dados, apenas

	parte deles, porque não há condições para albergar aqueles dados todos, ou aqueles dados são sensíveis e não podem ser partilhados. Ou seja, as maiores preocupações são um pouco a mistura disto tudo. Eu trabalho com dados clínicos, onde existe muita sensibilidade à volta destes dados, e muitas opiniões. Opiniões que estes dados não devem ser vistos por toda a gente. Existem profissionais da opinião que os dados que registou não podem ser vistos por médicos do mesmo perfil, pois são confidenciais e apenas podem ser vistos pelo próprio. Mesmo quando são substituídos por um outro colega não querem que estes vejam os seus dados. Existe hoje uma maior preocupação em relação aos dados, que não existia há alguns anos. As tecnologias despoletaram esta questão, porque começamos a ter muita informação, que antes não tínhamos. Os sistemas hospitalares, neste caso de cuidados primários, evoluíram muito nos últimos anos, no que toca à informação que se regista e aos grupos de profissionais utilizadores. Estamos a tratar do processo para que os nutricionistas, por exemplo tenham acesso à PDS. Concordo que em relação à PDS deveria haver mais informação sobre as políticas de utilização de dados. Foi um grande passo, e os próprios embaixadores da PDS e outros profissionais já fizeram sentir esta necessidade. Antes de se dar outro passo de gigante, deveria de alguma forma parar-se, olhar bem para a situação atual e poder identificar e corrigir riscos existente.
P3.V1.1 – P1HES#01	A maior preocupação nestas situações é com a falha dos sistemas. A disponibilidade dos sistemas. Mais do que a segurança. A minha maior preocupação em termos da dependência de outros sistemas ou da dependência das redes informáticas, ou da dependência que os sistemas têm neste momento no domínio da saúde, é haver uma falha no acesso ao sistema. Se eu não tiver informação no hospital não tenho serviços, consultas.
P3.V1.1 – P2HES#02	Dentro da área da saúde o que me preocupa mais como utente são os meus dados clínicos. Acho positivo a partilha de dados com outras organizações de saúde, desde que esteja garantida a sua segurança. No caso da PDS não sei se o utente é informado sobre a utilização dos dados. No caso de utilização dos meus dados em estudos clínicos, deveriam perguntar-me se eu estou ou não de acordo, se não existir uma cláusula prévia de autorização dos meus dados. As maiores preocupações de funcionarem em rede têm a ver com a segurança da informação. É importante salvaguardar os dados, tanto na componente de rede de comunicação entre instituições, como nos dados que circulam na rede e na forma como circulam na rede. A passagem de dados não encriptados pode facilitar o acesso a estes dados. Tem que haver uma confidencialidade dos dados, temos que saber quem é que acede ao quê. Têm que existir *logs* sobre tudo o que foi feito, no sentido de responsabilizar as pessoas – a parte humana que nós não conseguimos controlar.
P3.V1.1 – P2HES#03	Nós tentamos ao máximo isolar um serviço, mantendo as portas necessárias para trabalhar, por acesso remoto para acederem à informação que esse serviço tem para partilhar. Isto dentro do hospital. Para fora a ideia é a mesma, mas temos que pensar primeiro o que podemos passar para fora e o que é necessário para o exterior. É o caso das análises dos doentes. A segurança assim uma das maiores preocupações. E hoje em dia já estamos a pensar nos dados que estamos a passar para o exterior. Até há bem pouco tempo o hospital não passava nada para fora. A única informação que saía do hospital era uma imagem com um número de identificação, sem dados pessoais, que ia para um médico do exterior para análise e relatório. [...] Havia já uma preocupação em relação à proteção da privacidade do doente. Ainda hoje acontece assim.

P3.V1.2

P3.V1.2 – P1ULSNA#01	Sim, e julgo que começou a ser feito algo há dois anos com a criação de um grupo de trabalho, que entretanto parou, em que se estava a

	trabalhar em conclusões muito positivas, mas que entretanto parou, face à mudança das prioridades. Por um lado uma maior sensibilização. Porque enquanto algumas organizações podem estar mais preocupadas, outras podem não estar alertadas para as questões da segurança. Por outro lado uniformização, que permite que todas as organizações façam as coisas de forma semelhante, que sigam as mesmas regras, o que acabará sem dúvida por contribuir para a partilha de dados de uma forma mais segura.
P3.V1.2 – P2ULSNA#02	Sendo nos casos de segurança física ou lógica, A ULSNA tem uma estrutura de autenticação, *single sign on*, para aplicações sobre sistemas operativos Windows. Criamos uma VPN entre todas instituições do distrito sobre a RIS, colocamos equipamentos nosso, onde configuramos VPNs para todos os locais que pertencem à unidade local de saúde. Neste momento qualquer utilizador ou máquina, ao contrário de alguns anos em que não existia login, necessita de uma autenticação. Quanto à partilha de experiência entre equipas, nomeadamente em segurança, é desejável e já acontece. Acontece contudo de uma forma informal. Seria vantajoso fazer com que todas as instituições de saúde pudessem partilhar aquilo que é as melhores práticas ao nível de segurança e depois implementá-las numa forma organizada. Participei há dois anos atrás, convidado pelo ministério da saúde, no porto, numa equipa para estudar as boas práticas de segurança. Temos um documento muito extenso neste domínio, que aborda as boas práticas transversalmente, não olhando ao fabricante. Apresenta, para instituições deste tipo, aquilo que são as regras base em termos de segurança. Temos contudo um problema na área da saúde com alguns anos que tem a ver com a autenticação dos utilizadores e aplicações. Durante alguns anos o ministério da saúde não deu resposta às solicitações tecnológicas locais e cada instituição seguiu o seu próprio rumo neste domínio. Este documento tinha por objetivo, independentemente dos equipamentos adquiridos, definir regras base que se devia seguir.
P3.V1.2 – P2ULSNA#03	Não é fácil uma padronização das medidas de segurança nem na forma de agir. Agora caminhar neste sentido, um padrão vai exigir que todas as instituições tenham basicamente os mesmos sistemas de segurança. Como efeitos práticos, no domínio da segurança, e olhando sempre para o lado do utente, este sai beneficiado.
P3.V1.2 – P1USF#01	Sem dúvida, facilitaria imenso a proteção de dados.
P3.V1.2 – P2USF#02	As questões da segurança da informação terão de ser sempre colocadas. Não podemos estar a pensar que vamos colocar um serviço numa plataforma, sem pensar que seguranças vamos ter em relação a esse serviço. Temos que pensar muito bem no desenho de toda a plataforma. Inclusive coloca-se a questão que tipos de dados vamos partilhar: dados clínicos, dados não-clínicos, dados de backoffice? Para todo este tipo de dados estas questões são todas colocadas e discutidas, porque existem locais específicos para colocar este tipo de dados.
P3.V1.2 – P1INEM#01	É necessário uma maior interoperabilidade ao nível da segurança que suporte a partilha de experiências, promover uma padronização daquilo que são as melhores prática e acima de tudo aproveitarmos o que está feito, e até inclusive aprender com as más práticas. Esta colaboração poderia também chegar à partilha de incidentes, vulnerabilidades, em que toda a gente fica informada e tenta corrigir. O ministério da saúde é suportado pela RIS e o INEM tem um link para esta rede. Em termos práticos poderia fazer-se com que existisse um domínio de confiança mais alargado entre estas instituições. A existência de uma rede própria, em que não estamos dependentes de um fornecedor de serviços, mais fácil seria alinhar políticas de segurança, e até para definir normas de interoperabilidade entre os vários organismos. Neste momento com os hospitais apenas conseguimos enviar informação através de correio electrónico, que depois é anexado ao processo do paciente, o que não é seguro. No futuro teremos que caminhar para uma maior interoperabilidade.
P3.V1.2 – P2INEM#03	Sim, só com a experiência de vários é que se consegue padronizar.

	No caso do INEM a nossa infraestrutura de segurança foi instalada com base na experiência de empresas externas, o que faz com que não consigamos ter um controlo total sobre tudo o que está instalado de momento. Lança-nos algumas questões e problemas internos que já discutimos, e não temos o conhecimento suficiente internamente para abordar o tema da segurança e garantir segurança em 100% em tudo o que fazemos, até no que fazemos com outras organizações. Nesta situação é um problema alinhar politicas de segurança com outras organizações.
P3.V1.2 – P2INEM#04	Com certeza que sim. O efeito prático é percebermos muitas vezes na realidade, que na prática podem existir circunstancias que torna estas situações muito mais sensíveis, e que nós muitas vezes não sabemos como é que as coisas são utilizadas. Por exemplo, se nós nos referirmos aquilo que são os nossos dados mais sensíveis, mais vulneráveis neste sentido, perdemos um pouco a ideia de como eles são utilizados na rua. Quando vimos a saber como é que eles chegam ao hospital, como são utilizados no hospital, por vezes somos obrigados a repensar a segurança destes dados, sob pensa de sabermos que esses dados podem ser utilizados incorrectamente. Na prática seria possível o alinhamento de medidas de segurança entre as organizações. Dou-lhe um exemplo concreto – no âmbito da PDS, nós sabemos que temos serviços que entregam um conjunto de dados, mas depois não sabemos como é que eles são utilizados, e portanto digamos que o nível de segurança poderia ser maior ou menor com base neste intercâmbio desejável. Teríamos todos, vantagens se existisse mais informação sobre segurança quando as organizações partilham dados e serviços. Tanto nós como quem vai utilizar os dados.
P3.V1.2 – P2INEM#09	Absolutamente, porque se houvesse um padrão que todos tivessem que seguir, relativamente a medidas a tomar, sejam de segurança de dados, sejam de instalações, sejam de redes de comunicação, seria muito melhor do que cada instituição ter os seus próprios métodos. Se alguém que tem mais experiência passar este conhecimento a outros, todas as organizações lucram, pois de experiências várias, se vai tirar o que de melhor existe, e criar uma norma única. Produzia-se um domínio de confiança maior. Cria-se uma confiança maior entre as instituições que depois suporta melhor a partilha de dados.
P3.V1.2 – P2INEM#10	Sim é desejável uma maior colaboração. Até porque um dos maiores problemas ([…]) é mesmo a falta de comunicação, de colaboração, a falta de interajuda, de interligação, que deveriam ser transparentes e transversais. Repete-se muita informação, o que aumenta o risco da confidencialidade, e muitas com breves diálogos conseguia-se resolver problemas que são graves. Na prática se houvesse uma preocupação maior de colaboração entre os responsáveis de sistemas, em partilharem aquilo que são as melhores soluções, na prática, evitava tempos elevados de desenvolvimento, replicação de dados, simplificava a atualização dos dados, e na realidade tornava mais fácil a sua segurança. Muitas vezes neste domínio as organizações vão buscar soluções ao exterior, por falta de recursos especializados, e acredito pela simplificação do desenvolvimento.
P3.V1.2 – P1HFF#01	São questões de interoperabilidade técnica e também organizacional. A partilha de dados entre instituições depende de uma interoperabilidade não-técnica aos níveis da segurança, da protecção de dados, protocolos de entendimento.
P3.V1.2 – P2HFF#02	Sim é possível e muito importante. Ajuda-nos a fazer uma melhor gestão da mudança. Se quisermos alterar para um novo sistema, a interoperabilidade não é só com outras instituições, também é interna. Se tivermos um bom plano de interoperabilidade interna, ajuda-nos na interoperabilidade com outras instituições. Vai sem dúvida ajudar no processo de gestão da mudança.
P3.V1.2 – P2HFF#03	É desejável que haja aqui uma colaboração [interoperabilidade não-técnica] em assuntos como a segurança, a proteção e a privacidade de dados que suporte depois este contexto de colaboração. O objetivo é que depois a tecnologia consiga garantir o paradigma da informação e do acesso à informação. Porque neste caso o sistema como está montado não vai de encontro a este desígnio. Também

	não é claro em termos médicos, quem deve ou não deve ter acesso à informação. Antes mesmo de termos o paradigma tecnológico a responder há várias questões que não são claras. Dou-lhe um exemplo: se eu vou informatizar uma cardiologia, ou uma medicina 2, teoricamente em termos de informação a estrutura de dados é igual, mas existem muitas discussões que me dizem que na cardiologia existe muita especificidade.
P3.V1.2 – P1SPMS#02	Não vejo desvantagens nesta partilha de soluções e colaboração. Apesar de ter um efeito quase invisível, as pessoas tendo a perceção de uma melhor segurança, as pessoas sentem-se mais confortáveis na utilização dos sistemas e na troca de informação. O efeito é mais esse. Neste momento as pessoas preocupam-se com a possibilidade de furto de dados na área da saúde, apensar de em Portugal ainda não se terem verificado casos graves. Sabemos que há interesses ocultos por parte das farmacêuticas, seguradoras, em utilizarem os nossos dados. A nossa sorte é que nesta fase ainda estamos bem protegidos através da RIS. Se alguma instituição "abrir as portas para alguém entrar lá dentro" e aceder a esta rede, a RIS, aí temos um problema, pode ficar tudo comprometido.
P3.V1.2 – P2SPMS#03	Eu julgo que sim. Os efeitos práticos são muitos. Temos casos reais de práticas de envio de imagens clinicas, relatórios, em que são partilhados dados clínicos, em que é necessário que sejam tomadas todas as medidas de proteção de dados. É nossa preocupação que o mecanismo de comunicação e o canal de comunicação sejam seguros e que respondam a processos de segurança. Agora faltam as outras camadas, nomeadamente as aplicações.
P3.V1.2 – P2SPMS#04	Sim. O CAIC (comissão de acompanhamento de informação clinica) é um bom exemplo desta colaboração. Tem vários grupos de intervenção. Partilhar experiências, entre organismos nacionais, para que a segurança de infraestruturas possa andar ao lado da segurança da informação. A passagem de conhecimento é sem dúvida o efeito prático mais evidente que pode resultar da colaboração entre instituições, assim como a passagem de tecnologias, processos e *standards* usados, os bons e os maus resultados. Os próprios custos podem diminuir, uma vez que já alguém fez um determinado passo e pela experiência obtida já estão mais avançado, já fizerem o estudo. Porque não ouvir e passar este conhecimento a outros? Deste modo muitas instituições não necessitavam de começar do zero.
P3.V1.2 – P1HES#01	Eu acho que em todas as matérias que digam respeito aos sistemas de informação, às normas e às regras, deveria de haver mais colaboração entre estes profissionais. No suporte aquilo que é a privacidade dos dados, uma partilha de experiências era de todo uma mais-valia.
P3.V1.2 – P2HES#02	Quanto a mim uma das lacunas existentes ao nível da segurança, tem a ver com o facto de as instituições utilizarem diferentes *softwares* para o acesso a uma plataforma geral. Aqui temos alguns pontos de falha. Em termos de interfaces existem muitas falhas. Quanto maior for o número de aplicações para o acesso a esta plataforma geral, maiores vão ser as falhas. Até porque depois cada um terá um desenvolvimento específico. O ideal era existir uma uniformização dos sistemas de informação, com diretrizes vinda do ministério da saúde, no sentido definir prioridades de uniformização. Por outro lado o próprio sistema ficava mais fechado, porque atualmente são empresas externas que fazem a manutenção das aplicações, com bases de dados que guardam muitos dados. Uma maior colaboração é assim essencial a esta uniformização. Qualquer profissional que transita-se de uma instituição para outra saberia trabalhar nas aplicações, uma vez que seria semelhante em todos os hospitais. Atualmente existe uma dificuldade quando um profissional de movimenta entre instituições, dada a diferença entre aplicações.
P3.V1.2 – P2HES#03	Dentro do hospital temos apenas uma equipa com técnicos vocacionados para determinadas áreas ou valências. Em alguns hospitais existem várias equipas. Na área da segurança não temos tido situações de colaboração com equipas similares de outros hospitais. Temos tido sim na área de redes, na área de bases de dados, nomeadamente com o hospital de Portalegre. Em situações onde temos

	menos conhecimento é fundamental a colaboração. Temos uma colaboração com a SPMS no campo das bases de dados. A segurança informática dependeu muito da nossa formação. Fomos um bocado autodidatas. A área da segurança ainda é uma lacuna muito grande ao nível dos hospitais. Acabamos por estar salvaguardados pela RIS. Empresas com as quais tínhamos contrato, ajudaram nesta questão. Foi um conhecimento essencial na fase inicial. Uma vez que a segurança é um pilar fundamental à proteção de dados, tem que haver um investimento maior nesta área. Um investimento não só em termos físicos, mas também em termos de conhecimento. A maior lacuna atualmente é a formação.

P3.V2.1

P3.V2.1 – P2ULSNA#02	Houve apenas um projeto desenhado em equipa, documentado, para a segurança física da infraestrutura interna e rede de VPNs. Temos dois perímetros de segurança. Foram definidos os riscos e pessoas autorizadas. A nível dos utilizadores e aplicações, temos um problema que resulta de aplicações com 20 anos (SONHO e SINUS), sobre ORACLE 7.3.4, em que já não existe apoio técnico. Os próprios *updates* de segurança do próprio fabricante são um problema. Sistemas que ainda carecem de acessos via TELNET, sendo que a interação de dados não é problema.
P3.V2.1 – P2ULSNA#03	De certa forma sim, somos cuidadosos em relação aos riscos. Apresenta como vantagem o facto de podermos ser mais concisos.
P3.V2.1 – P2USF#02	As políticas de proteção de dados devem ser sempre desenhadas com base naquilo que é a análise do risco. Na ARS desde que existe o *datacenter*, cumprimos metodicamente todo o desenho da rede. Até porque se não cumprirmos nada funciona. A análise do risco realizada é orientada à infraestrutura e á informação. Se orientarmos esta análise apenas à infraestrutura e não tendo em conta a informação, as aplicações não vão funcionar da mesma forma. Tem que existir uma noção muito clara do projeto, que tipo de informação utiliza, quais os tipos de dados, a criticidade dos dados, e saber o circuito deles. A privacidade dos dados deve ser encarada como uma questão de risco. Apesar de ainda não ser uma realidade, estas questões devem vir gradualmente a ser integradas na análise de risco. É muito difícil fazer passar esta informação. As organizações trabalhavam a um nível só, no máximo a dois níveis. Segurança apenas. E é muito difícil que estas percebam que é necessário trabalhar em outros níveis. Os próprios parceiros de desenvolvimento, traziam as aplicações formatadas, e que com um servidor e um IP de rede estava tudo a funcionar. A realidade atual não é esta. Não pode ser esta. Tudo tem que ser pensado em vários níveis, porque senão as aplicações não vão funcionar ([…]). É necessário uma infraestrutura bem instalada, para poder posteriormente dar maior atenção à questão dos dados. Em alguns casos a infraestrutura é já um domínio que está a começar a ser bem trabalhado. Significa que em algumas organizações ainda vamos demorar algum tempo a chegar à camada de proteção e dados a sério.
P3.V2.1 – P2INEM#03	Não. A experiência que tenho, e não só no INEM, grande parte da estrutura está assente em empresas externas, ou seja, eu próprio não consigo fazer uma simples alteração num router, tenho que recorrer à empresa externa responsável. Mas isto não impede que haja uma análise do risco. Deveria caminhar-se para no futuro dar-se mais atenção a este requisito, a análise de risco, de preferência que pudesse evoluir mesmo para a protecção de dados.
P3.V2.1 – P2INEM#04	Não, não tem por base uma análise do risco. Estas coisas têm sido feitas mais pelo senso comum. Não há nada estabelecido. Agora concordo que uma análise do risco poderia contribuir para um desenvolvimento mais integrado dos sistemas quanto à segurança.

P3.V2.1 – P2INEM#09	Não, não foram baseadas numa análise de risco. Digamos que numa fase inicial, isto em termos de acesso a dados, não houve propriamente estudo nenhum. Sabia-se que determinadas pessoas que pertencem a um determinado grupo ou serviços podem aceder a determinado tipo de dados. É a política que ainda hoje, se segue, ou seja, as coisas estão mais ou menos divididas por serviços, dentro destes serviços pode haver tarefas específicas (é o caso dos recursos humanos, em que um grupo trata com vencimentos, e um outro grupo que trata com a assiduidade – estes dois grupos cruzam-se entre si, mas um outro grupo que trate da correspondência já não tem ligação com os outros dois). Quando os grupos por qualquer razão se ligam entre si pode haver partilhas comuns, de resto elas são fechadas. Agora, deveria haver uma análise de risco prévia para a segurança como um todo. Há medidas que foram tomadas, mas que foram sendo desenvolvidas à medida que foram surgindo as necessidades (numa adaptação contínua), e não através de um processo de raiz que identifica-se os riscos. Houve numa primeira fase a preocupação de salvaguardar acessos físicos, sistemas redundantes. Ao nível dos dados, pensou-se também nos riscos. Há algumas coisas que em teoria e numa fase inicial foram feitas de forma redundante, ou seja, posso ter um servidor de dados localmente que vai replicar informação para outros servidores remotos (neste caso em Coimbra), em que se falha um de um dos lados o outro repões a informação. Houve algumas preocupações, mas não existiu um estudo prévio de suporte.
P3.V2.1 – P2INEM#10	Não no nosso caso. A segurança é apenas uma preocupação de quem desenvolve as soluções. Quando desenvolvo qualquer solução sei que tem que estar seguro. Só que toda a segurança deveria nascer numa análise rigorosa do risco e deveria ser bem planeada. Temos soluções que são autênticas quebras de segurança. O que vale é que são muito limitadas em termos de utilização. Se fossem abertas a outros sistemas teria obrigatoriamente de se analisar o risco. Haveria coisas a alterar seguramente.
P3.V2.1 – P2HFF#02	Não, mas temos uma ideia dos riscos existentes e das vulnerabilidades. Mas não existe um documento formal. Reagimos perante uma situação e damos origem a algumas regras. A nossa maior preocupação é a disponibilidade e qualidade da informação. Não nos preocupamos muito com a segurança dos dados, porque muitas vezes acaba por ser um "empecilho" ao início dos sistemas. O que interessa é colocar os sistemas a funcionar. Não deveria ser assim. As políticas de segurança são do tipo reactivo e não proactivo. Agora é desejável que exista uma análise do risco que suporte as medidas de segurança, e que depois possam ser harmonizadas com outras organizações.
P3.V2.1 – P2HFF#03	A análise de risco deve ser preponderante a estas matérias. Mas nós não a exercemos. Em termos de maturidade o hospital ainda não está aí [na análise do risco]. Temos apenas uma comissão do risco clinico. As decisões de negócio são tomadas com base na actividade clinica de prestação de cuidados. Prescrever o correcto ao doente correcto. São estas as questões críticas. Agora esta decisão de negócio de que forma a que impacta em termos de risco isso é praticamente, não digo tabu, mas está muito longe da atenção dos actores. Sem dúvida que é um caminho a percorrer. Mas no nosso hospital, só recentemente é que iniciamos os procedimentos de gestão do risco na falência do sistema de informação. Ou seja, nós estávamos a zeros neste domínio. Nós e os outros hospitais, a maioria. Uma das razões é porque não havia informação para proteger, ou seja, existia em papel os procedimentos tradicionais. Quando iniciamos a informatização, este primeiro passo foi demasiado imaturo. Para muitos hospitais um "texto livre é um processo clinico" – não há de facto tabelas de informação padronizadas que me permitem seleccionar opções em determinados contextos, e depois poder comparar esta informação, fazer *benchmarking*, etc. Isto começa agora a existir e nós estamos a levar isto muito a sério. A partir daqui é que começam a surgir outras questões. Por exemplo no acesso à PDS, o facto de nós não termos o mesmo sistema que os outros hospitais incorre-nos num desafio, mas obriga-nos a ir por aí. Porque temos que enviar informação estruturada. Nós não damos acesso aos nossos sistemas como nos outros hospitais, em que acedo e vejo tudo, como médico. Mas, eu como cidadão se quiser ter acesso à

	informação que me interessa, que me é devida, não se calhar ao diário de um médico, ao episódio mas à nota de alta, na maior parte dos sistemas nacionais isto não é possível. Porque o perfil de acesso ou dava acesso a tudo ou não dá acesso a nada. No nosso caso tenho acesso a tudo isto. Posso perfeitamente construir um perfil na PDS para o utente, para o cidadão, em que ele acede ao conjunto de informação que eu tipifico. Porquê? Porque eu estou a dar-lhe informação estruturada. Portanto o 1º passo para a privacidade do nosso ponto de vista está em garantir a estrutura de dados. Se eu não tenho informação estruturada eu não posso garantir privacidade. É o tudo ou nada. Um dos pilares fundamentais desta questão da privacidade de dados é precisamente a maturidade ao nível da gestão da informação.
P3.V2.1 – P2SPMS#03	Ainda não é uma prática comum o desenvolvimento de práticas de segurança com base numa análise de risco, mas deveria ser uma realidade de construir com base no risco. Fazer uma análise do risco sobre qualquer sistema é fundamental, porque conhece-se as vulnerabilidades, consegue-se caracterizar o risco, e procurar-se resolver o risco. E isto numa situação em que o risco acontece é fundamental ter os caminhos traçados e pensados, e perceber qual é o real impacto do risco. Faz todo o sentido que esta questão da privacidade dos dados também tenha por base uma análise de risco. A privacidade e proteção são um risco, não na vertente organizacional, não na vertente financeira, mas diria que na perspetiva do cidadão, representa um risco. Se os projetos, no desenho tecnológico, *à priori*, fizessem um impacto de privacidade, uma análise de impacto sobre a privacidade, em relação aos dados que utilizam, a forma como os armazenam, o tempo que armazenam, na forma como os relacionam, se conseguissem minimizar a informação e os dados que recolhem na medida do que é estritamente necessário, provavelmente minimizavam o risco. Este tipo de abordagem seria fundamental. Pode ser uma das portas de entrada, pelo menos para conhecer o problema da privacidade dos dados. Conhecer onde existem os riscos.
P3.V2.1 – P2SPMS#04	Uma análise do risco no sentido de perceber os perigos da utilização dos dados, acho que sim. Esta questão da privacidade deveria ser tratada como um risco, faz todo o sentido, ser tratada como um risco. Os dados hoje em dia são um risco muito grande. Apesar de eu estar mais ligada ao acompanhamento de soluções que alguém já pensou em como vamos fazer. Os arquitetos já pensaram no assunto ou deveriam ter pensado. No caso do portal do profissional da PDS em que é possível aceder a um processo clinico numa outra instituição, neste momento vê-se o todo o processo clinico – isto é preocupante. É necessário pensar no risco destas situações. O acesso à informação depende apenas do perfil profissional.
P3.V2.1 – P2HES#02	Os procedimentos de segurança não nasceram numa análise de risco. Surgem do nosso conhecimento, com base naquilo que são alguns padrões de segurança e que têm que ser implementados. As políticas que são implementadas estão de acordo com estes padrões. É o caso das medidas de segurança aplicadas na criação de um novo login de acesso. Existem padrões que nós vamos seguindo. Agora se os seguimos da melhor forma, claro que não seguimos. Uma análise de risco poderia ser uma ferramenta excelente, embora nós já sabemos quais são os riscos. Temos que fazer uma análise de risco que em simultâneo inclua as infraestruturas e a organização, e os dados. Até porque já temos algumas medidas implementadas, esta seria uma ferramenta integradora.
P3.V2.1 – P2HES#03	A análise de risco não o é a 100%. Existe o conceito, é utilizado. O Conhecimento não é o suficiente, é necessário mais conhecimento [em análise do risco]. Seria vantajoso trabalhar com ferramentas de análise do risco e depois definir medidas de proteção e segurança. Gradualmente incluir a privacidade. Para conhecermos onde temos falhas, temos que primeiro identificar estas falhas, e depois procurar resolve-as. É uma área de colaboração com outras instituições, uma vez que o risco é muito parecido. Quando temos alguma tecnologia nova, procuramos contactar hospitais que já tenham esta tecnologia, esta experiência, para tentar não cometer os erros deles [conhecer os riscos associados].

P5.V4.1 – P1SPMS#02	No nosso caso a existência de *standard* sobre a temática da privacidade seria muito útil, para implementarmos nos nossos processos de privacidade. Porque cada um faz da forma acha que deve ser feito. Não existe nada que audite depois. Nós lemos normas e boas práticas, mas são insuficientes. Mesmo a nossa análise do risco é focada na segurança da informação apenas.

P3.V3.1

P3.V3.1 – P2ULSNA#02	Como é óbvio a identidade digital é importante para o futuro da partilha de dados. Há uma evolução, pela qual nós temos lutado, tendo em conta que grande parte das nossas aplicações é desenhada pelo próprio ministério da saúde. Dentro das próprias equipas do ministério da saúde nunca houve um entendimento em relação a uma autenticação única. Um exemplo, temos o SONHO que tem uma base de dados própria par autenticação, temos o SINUS que tem a sua própria autenticação, temos a antiga aplicação de aprovisionamento que tem a sua própria autenticação, o sistema clinico, neste caso o SAME, com autenticação distinta e sem confiança entre estes sistemas. É necessário um *username* e *password* distintos para cada um destes sistemas. Nem todas as aplicações têm a segurança que deveriam ter neste domínio. Temos sistemas, que por exemplo, não encriptam *password*s, como temos sistemas que dependem das passwords ao nível do sistema gestor da bases de dados (como é o exemplo do ORACLE). Ou seja, se nós tivermos 10 aplicações temos 10 sistemas de autenticação diferentes e proprietários. Pelo menos ao nível das aplicações do ministério da saúde deveria haver uma preocupação em desenvolver uma autenticação única para todas as aplicações. Isto é extremamente importante. Contudo nos últimos dois meses está a acontecer um exemplo interessante, que é a passagem do SAME e do SAPE para uma nova plataforma denominada SCLINICO, que consoante o perfil de cada profissional têm acesso à área que lhe pertence. Ou seja, provavelmente, não por questões de segurança, mas sim de controlo de receituário, a autenticação evoluiu, prevendo-se a autenticação via cartão de cidadão ou cartão da ordem dos médicos. Ou seja o profissional é univocamente identificado. Penso que o cartão do cidadão não deveria ser utilizado apenas neste ato de autenticação, mas ser utilizado no acesso a qualquer aplicação. Seria uma forma única de identificar o individuo, universalmente e de uma forma segura.
P3.V3.1 – P2ULSNA#03	Temos vários sistemas de autenticação. Aqui já concordo com a uniformização de processos ou sistemas, para que em termos de comunicação a interoperabilidade não seja tão complicada. Independentemente de depois dentro de cada instituição haver outros sistemas para os utilizadores locais. Temos uma série de aplicações que acabam por complicar a ligação de dados. O ideal é que todos estes sistemas evoluíssem para um sistema único, centralizado. Apesar dos problemas de segurança estamos a caminhar para que os sistemas de autenticação confiem uns nos outros. É o caminho, o RNU, a PDS caminham para tudo mais centralizado.
P3.V3.1 – P2USF#02	Pode não ser completamente preponderante. É um dado a ter em conta. Acho que faz sentido que cada vez mais trabalhemos no caminho de uma base de dados única. Não é uma base de dados única onde tudo esteja concentrado. Os dados de identificação deveriam estar num local onde todas as bases de dados bebessem. Em que sempre que houvesse uma alteração, todas as instituições tinham acesso à informação atualizada. Não faz sentido a duplicação de dados existente na atualidade. Para mim, identidade digital significa um único local onde todos os dados do cidadão estivessem armazenados, e onde todas as instituições e os seus sistemas de informação a consultassem quando necessário. Quanto aos sistemas de autenticação, apesar de tecnicamente não ser uma questão fácil, e de eu não ser apologista de que tudo deve

	estar num único local, estes deveriam evoluir, com toda a certeza, com que o conseguíssemos fazer com base num único local. A existência de múltiplos sistemas de autenticação dificulta inclusive a mobilidade de profissionais. Os dados de identificação estão replicados por múltiplas bases de dados, e provavelmente diferentes em todas estas bases de dados. Deveria haver uma maior interoperabilidade entre estes sistemas. Não faz sentido, haver um identificador para a saúde, outro para a finanças e assim sucessivamente.
P3.V3.1 – P2INEM#03	São discussões que já tivemos. Em questões de tratamento de dados digitais como é que se poderia garantir, até em simples publicações digitais, que são cumpridos os direitos de autor, e que não há uma distribuição abusiva desses mesmos materiais. Podemos aplicar este conceito aqui. É preocupante quando um profissional de saúde, por exemplo, num sistema tem umas credenciais de autenticação e num outro sistema apresenta credenciais diferentes. Se as instituições estão a partilhar dados deverão evoluir para um sistema unificado de identidade. Poderia trazer vantagens. Vamos pensar que se todos tiverem sempre a mesma identificação, com base num sistema único e centralizado, a questão da interoperabilidade seria facilitada certamente, porque estávamos a trabalhar todos sobre o mesmo contexto e não contextos diferentes que obrigatoriamente depois têm de se relacionar entre si. Não chega partilhar dados, é necessário também partilhar a identidade digital, acamada de autenticação.
P3.V3.1 – P2INEM#04	Era desejável que estes sistemas evoluíssem para um sistema único ou que pelo menos comunicassem uns com os outros. Esta manta de retalhos não será suficiente, e a prova disso é que nós vemos que tudo isto representa uma tremenda fragilidade. Ainda que, e como a experiência nos diz, tudo isto pode ser mal utilizado, ou seja pode ser violado. Havendo um único sistema que gere a identidade digital de todos os profissionais, estamos a caminhar para um ambiente mais seguro, mas pode não garantir uma protecção de dados mais eficiente, poderá eventualmente ser mais problemático.
P3.V3.1 – P2INEM#09	Hoje em dia não se consegue "sobreviver" sem uma identidade digital. No INEM é extremamente importante em dois ou três serviços muito específicos. Em alguns o profissional necessita de um cartão que identifica o utilizador que vai enviar dados para o banco de urgências de um hospital. E aqui ele só consegue aceder ao serviço utilizando este cartão. Quanto à sua evolução, já há algum tempo que defendo, a identidade digital deveria ser tratada de um outra forma. A autenticação da pessoa, não deve servir apenas para autenticar a pessoas, mas também para a poder responsabilizar pelo que fez durante o dia. Isto por questões de segurança. Se por qualquer razão um profissional se lembra de dar a sua *password* a outro, não se consegue provar quem foi na realidade o responsável. Faz sentido, evoluir-se para um sistema único dos utilizadores, que permita abranger todas as organizações. Se pensarmos que por exemplo os profissionais de enfermagem mudam com muita regularidade de organização, mais do que os médicos, poderia fazer-se com que o sistema os acompanha-se.
P3.V3.1 – P2INEM#10	Quanta mais vezes eu tiver que me autenticar, de quantas mais contas de utilizador eu precisar, maior vai ser o risco de segurança, porque maior é a probabilidade de repetir e simplificar as palavras-passe. Deveria evoluir-se para um sistema o mais único possível, em que a minha autenticação seja comum a todos os sistemas. Seria no fundo um nível tecnológico de suporte a um domínio mais seguro, para partilha de dados.
P3.V3.1 – P2HFF#02	Na minha opinião deveria começar por haver um sistema de autenticação central. Neste caso através de SPMS. Há cerca de um ano iniciamos um projecto interno sobre gestão da identidade a nível interno, no sentido em que todos os colaboradores do hospital tenham acesso aos sistemas, mediante informação que existe nos recursos humanos. Gostaríamos que isto existisse a nível central, seria um facilitador. Ao nível local existe já alguma interoperabilidade a este nível. Uma única identificação que dá acesso a múltiplas aplicações é já uma realidade. O que defendo é no futuro haver também uma interoperabilidade entre estes sistemas a nível nacional. É o conceito de federação. Veja-se o caso dos estagiários que se movimentam entre os vários hospitais, em que é difícil fazer a gestão da sua

	identidade digital. Com uma gestão centralizada era muito mais simples. O próprio controlo do que é que cada um faz ficava facilitado.
P3.V3.1 – P2HFF#03	No passado a identidade digital era um dos principais problemas, que recebia as maiores criticas dos utilizadores. Basicamente não havia uma identidade uniforme ao longo do sistema de informação. O sistema de informação tinha múltiplas identidades para o mesmo ator em função do *subset* a que acedia. Nós aqui criamos uma política, temos feito um esforço grande, em que o mercado às vezes não ajuda, de garantir que o mesmo acesso, a mesma identidade digital acede a toda a informação a que tem que aceder. Isto para garantir a rastreabilidade dos dados. É necessário garantir uma identidade digital uniforme em todo o sistema de informação. Se saímos do hospital necessitamos de garantir – ainda agora ouço uma crítica dos clínicos que para fazer uma prescrição no sistema de prescrição nacional (PEN), têm outro login – é necessário federar a identidade digital. Criar aqui uma estrutura em que fosse possível ao clinico, uma maior transparência em relação à sua identidade digital – ou seja, ele tem a sua identidade, que pode ser uma identidade que em vez de ir de baixo para cima, pode vir de cima para baixo. Se o profissional de saúde trabalha em mais de uma instituição, e cada vez este potencial vai ser maior, para mim a identidade digital no SNS deveria ser única e era cedida pela ordem em ligação com o sistema central. Ou seja, deixava de haver o login do hospital e sim o login do domínio SNS.pt e que depois vinha por aí a baixo. Eu ia buscar essa identidade e federava este login aqui, que era igual, e esta pessoa era reconhecida na PDS, na PEN, nos subsistemas da instituição ou em cada um dos hospitais para onde fosse. É um dos pilares fundamentais para aquilo que será posteriormente a monitorização da privacidade dos dados. Sem isto (a identidade digital) é impossível garantir uma visão agregada, se a identidade digital não for única no sistema, e para mim o sistema é o SNS. Existe aqui um sério risco que pode comprometer aquilo que é a segurança futura dos dados – é necessário esta malha de identificação. Eu não sei como é que se vai rastrear que aquele médico deu aqueles Óbidos, fez aquelas prescrições, acedeu à PDs, se eu não conseguir saber que é ele mesmo! Facilmente. E neste momento há este trabalho a desenvolver. Em todos os subsistemas existe uma identidade digital diferente. Que nós nem sequer controlamos, nem sequer rastreamos. Funcionam como uma caixa negra. Nós não lhe temos acesso. Não conseguimos auditar. Ou seja, se quisermos ter uma visão agregada é difícil. Isto porque nós só controlamos o interior do nosso sistema. É possível saber aquilo que temos dentro mas temos muita dificuldade sem saber quando os dados saem para fora, ou quando temos que adotar um sistema externo, e depender dele. No 1º ponto onde eu falei em coerência e semântica da informação, mas também tudo o que tem a ver com a estabilidade e o próprio suporte do sistema. São aspetos que deixam de estar sobre a nossa alçada. E portanto a fiabilidade a estabilidade, etc. já não depende de nós. Existe o risco da proteção de dados quando eles são partilhados. O facto de internamente não podermos fazer nenhum escrutínio impede-nos de garantir seja o que for.
P3.V3.1 – P2SPMS#03	A identidade digital é a nossa base de subsistência. Conheço bem a dificuldade que é, e que tem sido no nosso universo conseguir caracterizar os nossos utilizadores com alguma qualidade. Ainda estamos muito longe de uma federação ao nível da identidade digital para o ministério da saúde. Cada entidade tem os seus processos de identificação, com a utilização de mecanismos mais ou menos seguros. Mas o problema maior é que as aplicações estão a tender a ser centrais. E portanto quando passa do domínio local para o central, significa que extravasa aquilo que é o mecanismo de identificação local, em que vê a pessoa e até pode verificar alguma da sua documentação. Em que tem acesso à área dos recursos humanos e consegue verificar se a pessoa é realmente contratada o não pela entidade. E agora passa a ter que transportar isto tudo para o mundo digital, em que nós centralmente, que fazemos gestão de aplicações, não vemos o utilizador final. Ao nível central são milhares de utilizadores, ao passo que no nível local estamos a falar nas dezenas e eventualmente centenas. Passamos do paradigma controlável para o paradigma nacional em que não existem mecanismos robustos. É O SANTO GRAAL. É uma questão difícil. Os modelos em si podem ser distribuídos, centrais, federados. Face a nossa dimensão nacional, acredito que é possível ter um modelo centralizado, ainda que depois possa fornecer serviços a outras aplicações ou sistemas

	locais. Como cada entidade tem a sua autonomia, depois os mecanismos usados para a identificação não são os mesmos. Daí eu não acreditar na hipótese de federação para a identidade. O modelo de gestão para a identidade que eu defendo, acaba por identificar o utilizador final muito com base naquilo que é a sua origem. Já o fizemos no processo das vinhetas, para os médicos, em que foi desenhado um processo em conjunto com a ordem dos médicos, que permitiu cruzar dados entre três entidades, para conseguirmos ter a certeza que num processo de registo, que a pessoa que se está a autenticar, do ponto de vista eletrónico é quem diz ser. É um dos processos do mecanismo de identidade digital, em um dos mais importantes. Os entraves ao desenvolvimento de sistemas de identidade conjuntos são mais organizacionais do que tecnológicos. A tecnologia a este nível já não é um problema.
P3.V3.1 – P2SPMS#04	Um dos problemas é que temos autenticações muito diversas. Dever-se-ia evoluir para uma única forma de autenticar o profissional. Estamos a evoluir neste sentido, para que a autenticação seja feita a partir do cartão do cidadão ou até através do cartão das ordens. Estão a ser testadas soluções centralizadas. Face à heterogeneidade dos sistemas, deveria evoluir-se para uma autenticação igual, um sistema único, e uma única autenticação ser o suficiente para utilizar várias aplicações, mesmo que noutra instituição. A mudança de sistemas não deveria obrigar a uma nova autenticação mas apenas à validação da autenticação anterior. Cada vez mais temos profissionais em mobilidade hospitalar, e nas ULS os profissionais de manha trabalham num hospital e de tarde num centro de saúde.
P3.V3.1 – P2HES#02	Isto hoje é uma malha de instituições. Para além de uma uniformização de um sistema de autenticação, temos que ter uma política de autenticação forte – como são o uso da retina, biométricas. Um login e uma *password* hoje não são seguros. Não garantem uma autenticação segura da pessoa. A utilização do cartão de cidadão, com os pedidos de pin do próprio cartão. Ou seja, ter mais que um mecanismo de autenticação. Deveriam também estes sistemas muito heterógenos falar entre si. Mais uma vez a questão da uniformização de sistemas. Caminhar-se para um sistema único a nível nacional que autentica-se os profissionais.
P3.V3.1 – P2HES#03	Em termos de identidade digital, qualquer pessoa que trabalhe neste hospital e vá para outro, tem duas identidades. O único ponto comum é o número da ordem dos médicos. Porque aqui utilizam um método de autenticação para aceder ao computador, outro para acederem à aplicação [neste caso o ALERT], e quando passa para outro hospital utiliza outros métodos de autenticação para as mesmas tarefas. É possível uniformizar os métodos de autenticação, com base em dados dos médicos centralizados, neste caso na SPMS. Não estamos a falar dos dados do doente. O caminho é um sistema centralizado de autenticação. Sentimos muito a necessidade, pelo menos internamente, de uniformizar a identidade digital entre todas as aplicações. Algumas tecnologias, aplicações, ainda não permitem a partilha de dados de identidade digital e autenticação. Cada uma tem as suas regras de autenticação. A utilização dos dados de autenticação ainda é um problema. Já batalhamos contra isto e desistimos. Já chegamos a ver os dados de autenticação usados para abrir várias sessões de utilizador [no ALERT]. Até no mesmo computador isto acontece. É necessário educar as pessoas, sensibilizar as pessoas [para uma boa utilização dos dados de autenticação].

P3.V4.1

P3.V4.1 – P2ULSNA#02	Independentemente do tipo de sistemas que temos, alguns já antigos, a escolha de determinadas bases de dados, como em todos os sistemas, por mais segurança e barreiras que existam, a utilização primária é aquela que pode envolver mais riscos. Mesmo como um

	bom sistema para ataques internos ou externos, um utilizador com um perfil para determinado nível de dados pode transcrever informação que visualiza, ou copiar esta informação. Em termos secundários não existem situações de utilização secundárias destes dados. O RNU (Registo Nacional de Utentes), uma base de dados que está a crescer com toda a informação do utente, onde tem existido muito cuidado na qualidade dos dados, permite que o registo interno ao nível do SINUS ou SONHO tenham uma interação com RNU, quando existem dúvidas sobre um utente. Um exemplo, se um utente afirma que está isento de uma taxa, pode no imediato ser validada no RNU.
P3.V4.1 – P2ULSNA#03	A maior preocupação surge na transferência de dados. O envio de dados, aquilo que é enviado coloca algumas questões de segurança, apesar de estarmos a trabalhar numa rede segura. Muito sinceramente, penso que o foco principal de preocupações é a utilização primária.
P3.V4.1 – P2USF#03	É complicado ([…]). Só podemos facultar dados pessoais a instituições devidamente acreditadas. Os cenários de utilização secundária são cada vez mais comuns, mais preocupantes. Não acredito é que as instituições estejam a pensar nestes e a adotar medidas eficazes de proteção de dados. Se forem recebidas indicações superiormente que um conjunto de dados tem que ser entregue, as instituições não têm grande poder sobre estas situações. Imagine que vem uma diretiva superiormente a dizer, que estes dados devem ser fornecidos a alguém, as instituições cumprem. E é a nível superior que têm que ser ditadas as regras para proteção destes dados. É ao nível do ministério (através de alguém especializado em privacidade) que faz sentido que estas questões sejam analisadas de uma forma transversal para todas as instituições, para que todos trabalhem da mesma forma. Não podemos ter a ARS norte a trabalhar de uma forma, e o centro a trabalhar de outra forma.
P3.V4.1 – P2INEM#03	Quando os dados são apenas utilizados internamente estão identificadas as pessoas que podem e têm acesso a esses dados, e que têm os cuidados adequados para que estes não se extraviem. Agora a dificuldade está mais naquilo que é passível de circular no terreno e que pode ser visto, ser exposto. Apesar de nosso caso a utilização primária ser mais preocupante que a utilização secundária, tem que haver soluções, garantias para a utilização secundária, garantias que permitam, que tal como na primária, os dados não são violados. Na nossa realidade está muito contida à utilização secundária dos dados.
P3.V4.1 – P2INEM#04	Tudo depende dos contextos. Mas a segunda hipótese poderá ser aquela, que mais problemas poderá levantar. Tudo depende da natureza da própria informação. Deveriam ser pensadas medidas especificas para estes cenários, pois o prejuízo de uma má protecção será maior do que na utilização primária. Há que repensar todas as utilizações secundárias – tenho a ideia de que alguém que tenha que ter, que de acordo com a sua função, tenha que aceder a um conjunto de dados, está por inerência afeto a um dever de confidencialidade sobre aquela informação. Com base nesta condição temos muitas vezes acesso aos dados. Na administração de uma base de dados temos todos os dados disponíveis. Quando tenho vários programadores a trabalhar sobre um projecto, se elas têm que ter acesso aos dados para desenvolver o seu trabalho, e sendo necessário garantir a privacidade destes dados, a este nível sei quem são as pessoas que têm acesso à informação – a minha preocupação prende-se com a utilização indevida de determina informação ou precavermo-nos que determinadas pessoas possam, por não ter suficiente conhecimento sobre a utilização de um determinado conjunto de dados, destrui-los inadvertidamente. E aqui a protecção de dados fica em causa. Isto numa perspectiva de uso abusivo de dados para outros fins.
P3.V4.1 – P2INEM#09	Tendo em conta o conhecimento sobre o funcionamento interno, os principais problemas estão associados à utilização primária dos dados. Por questões que nos ultrapassam é muito comum os profissionais partilharem a sua password, o que colocar grandes risco. Se alguém sair da instituição pode haver a tendência de divulgação de determinadas coisas (dados). Nesta situação a conta do utilizador é bloqueada. Faço isto por minha iniciativa, e não com base em políticas de proteção de dados. Para a utilização secundária deveriam existir também regras bem definidas, porque no caso da saúde, coloca-se a questão dos dados do

	doente. Existe sempre um risco quando alguém está interessado em recolher estes dados, para diversos fins. E portanto deveria realmente haver um estudo sobre esta matéria, porque para mim é de facto um risco, que deveria ser mais protegido. Não se conhece muito bem a utilização secundária dos dados no domínio da saúde. A partir do momento em que os dados saem da organização, pode acontecer tudo.
P3.V4.1 – P2INEM#10	Pessoalmente, eu acho que os maiores problemas surgem na utilização primária, que estão associados principalmente aos problemas de utilização das tecnologias de informação. Normalmente quem faz utilização secundária dos dados tem a preocupação de preservar a identidade dos dados. Existe a este nível uma maior proteção. A utilização secundária normalmente é estudar os dados obtidos. Normalmente faz-se em volume, retira-se a identidade dos dados. Quem faz isto tem o cuidado de preservar a privacidade. Normalmente é alguém que já está habituado, treinado, preparado para. Elimina todos os fatores que possam colocar em causa a privacidade. Isto não elimina a necessidade de haver regras próprias para a utilização secundária. Até porque é preciso avaliar que tipo de utilização se vai fazer com os dados. Implica que haja regras e que as pessoas tenham o cuidado de perceber até que ponto aquilo pode eventualmente colocar em risco a privacidade dos dados ou não.
P3.V4.1 – P2HFF#02	Os maiores problemas de privacidade penso surgirem na utilização primária. Na utilização secundária, tudo depende da pessoa que está a utilizar os dados, mas normalmente não existem tantos problemas em relação à privacidade destes dados e das pessoas. Dependendo do objectivo da utilização secundária dos dados, também deveria existir normas para a utilização dos dados. É importante identificar o individuo que vai utilizar estes dados, o seu objectivo e os riscos associados. Tem que se ajustar a protecção com aquilo que é o objectivo da utilização [secundária] dos dados. Tem que existir medidas rigorosas para estes cenários, procedimentos para impedir que estes dados saiam fora do seu âmbito de utilização. Existe um certo facilitismo, apesar das medidas que têm sido tomadas. Se por um lado é difícil fornecer dados para o exterior é relativamente fácil fornecer dados para o interior – por exemplo se um médico necessita de dados para apresentar num congresso, nós fornecemos os dados sem protecção específica. Basta a autorização do director clinico.
P3.V4.1 – P2HFF#03	Temos muitos problemas com a utilização secundária, e é um assunto que está a ser discutido neste momento. Há um procedimento que vai ser agora desenhado com a direção clinica, direção de enfermagem, direção de produção especificamente porque a DGTI levantou aqui a legitimidade da extração de dados fora de qualquer perfil de acesso. Ou seja, a partir do momento em que é possível, para um congresso, para um projeto de investigação nacional ou internacional fornecer um conjunto de dados é necessário estabelecer um *workflow* que permita: 1º averiguar da legitimidade para dar estes dados, no sentido de averiguar se devo dar esses dados, 2º estou a dar os dados corretos, porque ao extrair da base de dados "em bruto", eu posso estar a tirar informação do contexto e da semântica em que eles foram registados, e portanto podem perfeitamente ser mal interpretados pelo investigador no momento em que os vai usar. Se a informação não for clara, à medida que a complexidade do registo aumenta a mesma informação está espartilhada, a sua utilização detora-se. Em relação à proteção e dados nestas situações a direção clinica e a comissão de investigação clinica dão um parecer em que assumem que o pedido de informação é legítimo para o contexto. De seguida é a direção de controlo de gestão a fornecer a informação. Para garantir que a informação sai sempre da mesma fonte de verdade, ou seja da mesma entidade. Também havia o risco de diferentes entidades dentro da organização tirarem a mesma informação e muitas vezes o resultado ser diferente, haver incoerências. Tem que existir uma única fonte de saída de informação, para que esta seja fornecida corretamente, contextualizada e para o fim a que se destina. E também para garantir a proteção da propriedade da informação e que a informação é utilizada apenas para aquele fim. É também exigido uma cópia do resultado final, para se perceber se de facto a fonte foi identificada e os dados foram utilizados de forma correta. Não temos ainda regulamentado, especificado em que contextos é que se aplicam medidas especificas como por exemplo a anonimização de dados. A questão tal como está, ainda está muito imatura. Ou seja, corremos muitos riscos. Podemos estar a dar informação a mais, não digo por negligência, mas por descuido, por desconhecimento. O facto de nós estarmos cada vez mais a

	partilhar dados em ambiente alargado pode vir a agravar-se aquilo que é a utilização secundária de dados. Porque a partir do momento em que eu tenho a fonte, e consigo aceder a esses dados sem perfil de utilizador, extraio os dados sem rastreabilidade, extraio os dados em bruto, sem nenhum controlo, é sem dúvida a maior lacuna em matéria de proteção e dados.
P3.V4.1 – P2SPMS#03	É uma pergunta difícil. Eu diria que podemos ter mais problemas talvez na utilização secundária. Incluindo aqui os processos de integração. Muitas vezes os sistemas são desenhados com um determinado objetivo, e depois aparecem um conjunto de integrações e também interoperabilidade à volta, que fogem do processo inicial. Se partirmos do princípio que os dados são do próprio cidadão, deveria haver, nos casos de utilização secundária, um consentimento eletrónico. Se existisse um consentimento eletrónico a autorizar a transferência dessa informação entre as diferentes aplicações, provavelmente era um primeiro passo para garantir que o fim para o qual os dados foram recolhidos era respeitado.
P3.V4.1 – P2SPMS#04	A utilização secundária pode ser mais preocupante. No nosso caso, nós disponibilizamos muitos dados a várias entidades para estatísticas, e são enviados todos os dados registados, existindo alguns cuidados com dados identificados. Agora eu não sei se estes dados não serão utilizados depois em outras explorações. Deveria haver um maior controlo sobre todos estes processos, uma vez que estes processos têm tendência a crescer muito.
P3.V4.1 – P2HES#02	Acho que em ambos os campos surgem problemas de privacidade. Cada um contudo com um grau de exigência diferente. Ou seja, em ambos é necessário e fundamental que existam garantias de que os dados foram aplicados e que só tenha acesso a eles quem esteja habilitado devidamente, tanto na utilização primária como na secundária. A utilização secundária preocupa mais no sentido em que alguém, que eventualmente, não deveria ter acesso a esses dados, conseguiu aceder-lhe. É necessário ter algum cuidado com estas pessoas, com os fins da utilização dos dados. É aqui que no meu ponto de vista poderão surgir mais fugas de informação. Na utilização primária, teoricamente serão as pessoas que trabalham com os dados, todos os dias, que estão mais conscientes da importância dos dados. No caso da saúde, numa utilização primária temos médicos e enfermeiros. Numa utilização secundária enquadro os administrativos, que por vezes têm mais privilégios do que deveriam ter, e podem passar alguma informação. Só confiamos dados com autorização do conselho de administração. Existem alguns processos de *data mining*, dados que são trabalhados principalmente para a área administrativa e financeira. Existe alguma preocupação na proteção destes dados. Não expor dados pessoais. Apenas quando o doente solicita estes dados é que lhe é disponibilizada informação mais detalhada. Mesmo assim é necessário ter mais cuidados com a utilização deste tipo de informação.
P3.V4.1 – P2HES#03	Se retirar os dados e não passar informação pessoal de identificação do doente não é problemático. Sempre que se cedem dados para estudos estatísticos não vai a identificação do doente. Apenas o básico, como a idade, o sexo, e pouco mais. Agora sempre que se extraírem dados tem que haver a aplicação de um conjunto de medidas de proteção, para garantir que o utente entra na estatística mas não se sabe quem é.
P5.V1.1 – P4SPMS#05	Acha que as instituições estão a trabalhar bem em situações de utilização secundária de dados? Algumas estão! Não dão nada a ninguém. Logo no entender delas estão a gerir bem os dados. Outras dão tudo de uma forma por vezes irresponsável, e talvez ilegal. A lei tem que acompanhar aquilo que é as necessidades do mundo. E se o mundo necessita de utilização secundária de dados, para investigação, para definição de perfis de risco, perfis de consumo, para otimizar alocação de recursos financeiros, então não é de todo irresponsável a sua utilização. Pelo contrário, até seria irresponsável não os utilizar. Se é ilegal é diferente. Ou muda a lei, ou é-se irresponsável por ir contra a lei. Mas a lei, arrisca-se a ser irresponsável, ao não permitira a evolução tecnológica na área da saúde, pela sua não evolução [...]. Um conceito fundamental, que não é necessariamente um conceito fácil de implementar, é a consciência

	progressiva que o doente tem, e que os doentes devem ter, das utilizações secundárias. É mais importante que a utilização anonima dos dados. Eu arriscaria dizer, que se calhar eu gostava mais que me perguntassem, do que utilizarem de forma anónima os meus dados. São dois caminhos. A utilização secundária dos dados pode optar por estes dois caminhos. Aquele em que a informação que se venha a obter traga um benefício para o doente em causa, obrigatoriamente não pode acontecer de forma anónima. Tem é acontecer de uma forma responsável. Acho que tem que haver alguma regulamentação, um pouco mais clara para estas situações [de utilização secundárias dos dados], tem que haver um enquadramento macro mais clarificador, no qual se foque os princípios mais do que as regras estritas, porque depois regras muito estritas nesta área, não são aplicáveis. É no campo dos princípios, como por exemplo este que falamos, "o benefício retroativo previsível" [...]. A partilha de práticas entre instituições só vai acontecer, eu só acredito nela, quando a instituição entender que isto é uma matéria importante, aloque alguém para se preocupar com o assunto, e ai a colaboração com outros responsáveis é possível.

P3.V5.1

P3.V5.1 – P2ULSNA#02	Esta pergunta não se deve fazer só aqui, mas a nível mundial. Não existe nada pensado neste domínio. Antes de chegarmos a este nível/ponto tem que haver uma monotorização dos sistemas. Não existe neste momento qualquer solução implementada. Mesmo havendo uma denúncia sobre um infrator dificilmente saberemos os dados afetados. A nossa monitorização é muito focada nos serviços (número de consultas/*queries* por minuto) e aos equipamentos. Trabalha-se muito na segurança física de dados, em planos de contingência para links primários, links de backup de dados, mas nada focado na privacidade dos dados. Mas tem que se começar a caminhar neste sentido.
P3.V5.1 – P2ULSNA#03	Sim, digamos que ao nível local é possível. Temos sistemas de *backup* que nos permite repor quase tudo. É conteúdo, tal como para a segurança, desejável haver planos de contingência para que se possa agir rapidamente se foi detetado a utilização indevida de dados. Mas sinceramente não sei como desenvolver este tipo de planos, nem que medidas deve conter.
P3.V5.1 – P2USF#02	Acho que sim, deveríamos estar-nos a posicionar ao nível dos dados. A perda de dados pessoais pode ser muito crítica. Se as instituições ainda não pensaram nisto deveriam pensar, faz todo o sentido. É uma daquelas questões pertinentes e que tem que existir nas instituições alguém que saiba responder a esta questão.
P3.V5.1 – P2INEM#03	Os planos de contingência neste ou em outro contexto têm que existir. Sim deveríamos também pensar em planos de contingência para os dados. Tal como numa infraestrutura, ter sempre um plano b, que nos dê suporte quando alguma coisa corre mal. Não conseguimos prever o que pode acontecer de um momento para o outro. Posso ter um utilizador mal-intencionado que elimina um conjunto de registos ou posso ter um utilizador bem-intencionado mas que inadvertido o faz, alterou um conjunto de dados. Por isso tem que haver sempre alguns planos de contingência, a garantia que se algo correr mal, se consiga recuperar ou reconstituir aquilo que tínhamos. No INEM não temos planos a este nível. Apenas *backups* de bases de dados. Não é nitidamente suficiente. É necessário pensar mais à frente. Prever todos os cenários que podem acontecer e procurar arranjar um plano para que, ou não aconteçam, ou que mitiguem e limitem os efeitos.
P3.V5.1 – P2INEM#04	Eu penso que sim, os dados são digamos o valor mais precioso que existe em qualquer organização ou em qualquer sistema. Por

	enquanto ainda estamos ao nível da disponibilidade dos sistemas. Ainda não estamos ao nível de situações de quebra de confidencialidade dos dados. Vamos ter que caminhar neste sentido. Apesar de nós aqui somos obrigados a pensar as coisas para lá do backup de dados. Existem processos que colocam a informação imediatamente disponível, caso falhe um dos sistemas críticos. Nos outros sistemas ainda não temos esta preocupação. Mas se houver uma quebra de confidencialidade num conjunto de dados os sistemas ainda não conseguem detectar esta quebra. Concordo que se deverá caminhar no sentido de se perceber a existência de quebras de confidencialidade e poder agir rapidamente, minimizando os possíveis impactos.
P3.V5.1 – P2INEM#09	Possível é! Os dados pessoais que nós temos, relacionados com doentes, em regra os doentes não são identificados. Não acompanhamos o estado do doente no pós-internamento. A menos que de alguma forma se consiga associar aqueles dados a uma identidade específica, aqueles dados não são atribuíveis a ninguém. Se se conseguir identificar uma pessoa com base nestes dados é possível prever algumas medidas de proteção para estas situações. Havendo uma ligação entre aquilo que o INEM faz e os hospitais, seria necessário estudar a forma de unificar todo este trajeto de forma a não haver violações da privacidade dos dados. Ou as tais possíveis violações.
P3.V5.1 – P2INEM#10	Desejável é sempre. Não me parece é que depois haja muita solução. Principalmente no caso de haver perda de dados. Se alguma informação de alguma forma se tornou pública, dificilmente vou conseguir ter um plano de contingência para isso. É desejável que haja nestas situações um plano de contingência no sentido de minimizar o impacto causado. Se houver uma fuga ou adulteração de dados têm que ser pensadas mediadas, que permitam proteger os visados. No nosso caso, é informação é editável num curto espaço de tempo, o que nos facilita esta questão. Num hospital onde houver uma fuga de dados sobre um grupo de risco é muito pior. O período de edição dos dados não é tão limitado como o nosso. Aqui é necessário muitos mais cuidados. Tem que haver medidas adaptadas a cada uma das realidades, a cada contexto.
P3.V5.1 – P2HFF#02	Já desenvolvemos um plano de contingência, uma vez que estamos totalmente dependentes dos nossos sistemas de informação, no acesso à informação. Definiu-se um plano em que são feitos *backups* locais internamente no hospital, por profissionais com autenticação local. Só que não existe grande proteção ao nível dos dados. Deveríamos estar a caminhar para o nível dos dados. Deveríamos ter um plano de contingência no caso da perda de dados. Ainda não temos plano a este nível. O processo clinico que nós temos por exemplo não permite eliminar dados. Permite marcá-los como erróneos, mas não permite eliminar. Havendo um furto de informação deveríamos ter um plano de contingência. Temos apenas os *backups* normais. Estes planos devem estar associados à identificação do risco que corremos e de alguma forma definir algumas tarefas que anulem este risco.
P3.V5.1 – P2HFF#03	Nós só agora, é que o hospital atingiu a maturidade para se preocupar com o plano de contingência para a falência do sistema de informação. É a prioridade. Se o sistema não estiver lá como é que eu registo informação. Como é que eu garanto a qualidade e a segurança da prestação de cuidados. E como é que a posteriori consigo inserir ou não os dados no sistema. Nós neste momento não temos instrumentos que nos permitam aferir de situações de dados adulterados, roubo de dados. Temos a auditoria clinica que é feita apenas à qualidade dos dados – saber se o campo foi bem preenchido, se o diagnóstico faz sentido. Em face do paradigma e do grau de maturidade em que estamos, em que 1º é necessário conseguir que os clínicos registem os dados, e depois aceitar que face à complexidade do registo, que aumentou, fruto da maturidade que nós queremos impregnar á qualidade dessa informação, coloca em causa segundo os clínicos a sua performance. Tudo o que tiver a ver com o "complicar" por razões de segurança, de qualidade, segurança clinica ou da informação, é ainda um processo de "evangelização que tem que ser feito". Agora o risco está a aumentar exponencialmente à medida que a qualidade de informação tem mais valor. Neste hospital eu asseguro que a qualidade da informação clinica electrónica tem um grau de nobreza que eu reconheço em poucos [hospitais].

	O facto de grande parte dos médicos exercer a sua atividade em várias unidades, publica e privada, induz aqui questões de segurança graves, e outras que nós não controlamos. Por exemplo na codificação, nós não controlamos se um médico em outro hospital, através da PDS acede ao meu hospital para ver informação clinica fora do contexto da PDS, e consulta diretamente o processo clinico do meu hospital. Esta informação pode ser prestada a terceiros fora do hospital. Não conseguimos controlar, validar e descortinar estas situações. Isto preocupa-me, o facto de um clinico em qualquer contexto, e pode estar a aceder ao processo clinico e a mostra-lo ou partilha-lo. Eu não consigo aqui através de mecanismos técnicos ter uma rastreabilidade a este nível.
P3.V5.1 – P2SPMS#03	Sim é possível. Sempre que existem falhas de segurança, que impliquem estar em causa os dados, isto é a proteção de dados, obriga a notificar os donos desses dados. Existem alguns mecanismos previstos para estas situações, em que sabemos que situações de violação de dados devem ser alvo de notificação. Mas do ponto de vista de segurança, não da informação. Mas se se conseguir agir antes do utente ser prejudicado, melhor ainda.
P3.V5.1 – P2SPMS#04	Para situações de furto de informação sobre grupos de risco, deveria haver planos de contingência. Deveria saber-se o que desenvolver no imediato. Tenho alguma dificuldade em identificar medidas práticas, pois não é a minha área. Ainda não temos furto de dados na saúde. Mas em relação aos nossos dados clínicos, nós temos aplicações instaladas nos centros de saúde de empresas privadas, com os dados em várias bases de dados. Várias vezes nós já questionamos o que é que estas empresas podem fazer com estes dados. Será que estas não vedem aqueles dados às seguradoras e farmacêuticas? Será que estas não cruzam estes dados com outras bases de dados? Todas estas situações deveriam ser identificadas, analisadas e acauteladas. Não será fácil.
P3.V5.1 – P2HES#02	Perante uma situação de violação e furto de dados, claro que sim, devemos ter um plano de contingência aplicado aos dados. Deveriam existir mecanismos que permitissem detetar este tipo de violação. Não sei se uma monitorização, se auditorias frequentes aos sistemas de informação. Tem que se ter sistemas que suportem este tipo de deteção e depois atuar. Imagine que alguém internamente pegava num conjunto de dados e os colocava na *cloud*. Tem que haver um mecanismo que detete esta situação, tem que haver uma prova. Para haver uma prova tem que haver alguém certificado na instituição (seria o ideal) que desenvolva estas tarefas. […] Hoje em dia já há algumas aplicações que fazem um registo detalhado das tarefas. Já chegam aos dados. Conseguem responder quem acedeu ao quê, a que horas e de onde. Exemplo, o ALERT não permite a um profissional apagar registos de informação. Mesmo se o profissional ter entrado no episódio errado e registado dados errados, este não os consegue apagar. É também uma questão de privacidade. É também uma medida de segurança para as pessoas que estão a ser tratadas ou atendidas. O diagnóstico não pode ser eliminado. […] Já se está a trabalhar nesse sentido, já com uma orientação para os dados.
P3.V5.1 – P2HES#03	Sim faz todo o sentido pensar-se em planos de contingência. Se os dados forem roubados convém haver um mecanismo para que eles não consigam ser vistos, nomeadamente através da sua encriptação.

2. *Data Reduction*

P3.V1.1	***Perfil 1** / Responsáveis pela implementação e coordenação da PDS*	***Perfil 2** / Técnicos e responsáveis pelos sistemas de informação*
Padrão encontrado Segurança Disponibilidade Dados Confidencialidade	"Segurança na disponibilização dos dados. A segurança começa a evoluir para a protecção de dados" (P3.V1.1-P1ULSNA#01)	"Já existem grandes directrizes em questões de segurança. Apesar da confiança na RIS, existe uma preocupação em relação à utilização dos nossos dados, [...], o que os utilizadores retiram " (P3.V1.1-P2ULSNA#02)
	"Numa rede de muitas organizações, milhares de utilizadores, a segurança é sem dúvida uma das preocupações prioritárias, assim como a disponibilidade dos sistemas. Para o utente a segurança dos dados é a maior preocupação " (P3.V1.1-P1USF#01)	"As questões da segurança são obviamente também uma questão importante. Ainda não existe muita sensibilidade para a privacidade dos dados, apresar de ser uma questão pertinente e importante " (P3.V1.1-P2ULSNA#03)
	"A rastreabilidade dos dados será sempre a preocupação maior. [...] São em simultâneo preocupações de segurança e de protecção de dados. A segurança é um dos primeiros patamares de preocupação " (P3.V1.1-P1INEM#01)	"Disponibilidade de serviços, utilizadores, utilização dos dados, suporte da RIS, [...] leva-nos a diferentes questões de segurança " (P3.V1.1-P2USF#02)
	"Um dos principias desafios é precisamente o que temos vindo a falar – os protocolos de entendimento, a parte da interoperabilidade" (P3.V1.1 – P1HFF#01)	"Primeiro a segurança, [...],e uma estrutura preparada para a protecção adequada dos dados. A confidencialidade [...]" (P3.V1.1-P2INEM#03)
	"[...] a questão da interoperabilidade é crucial" (P3.V1.1 – P1HFF#01)	"É a segurança, [...], das infra-estruturas de dados, [...], e gradualmente da segurança da informação " (P3.V1.1-P2INEM#09)
	"[...] as fontes de entendimento, do ponto de vista de processos, de informação, dos sistemas de informação, que se forem diferentes obriga a criar plataforma de integração tecnológicas próprias para eu passar dados, por exemplo de imagiologia" (P3.V1.1 – P1HFF#01)	"As maiores preocupações estão relacionadas com a forma de implementar as soluções. Aquelas que deveriam ser as maiores preocupações, [...], será mesmo a segurança da informação que circula. Da sua disponibilidade [...]" (P3.V1.1-P2INEM#04)
	"A acessibilidade da informação que é disponibilizada. Às vezes as instituições estão mais preocupadas em obter a informação do outro lado e nem tanto disponibilizar informação" (P3.V1.1 – P1SPMS#02)	"As instituições não estão habituadas a trabalhar em rede. Alguns conceitos não são compreendidos por todas as partes da mesma forma. Estes conceitos têm de ser alinhados. Nomeadamente a nível de processos" (P3.V1.1 – P2HFF#02)
	"A maior preocupação nestas situações é com a falha dos sistemas. A disponibilidade dos sistemas. Mais do que a segurança" (P3.V1.1 – P1HES#01)	"O hospital aqui faz um processo de uma determinada maneira, mas outro hospital faz o mesmo processo de uma maneira completamente diferente" (P3.V1.1 – P2HFF#02)
		"Os principais problemas estão relacionados com a interoperabilidade não técnica. A interoperabilidade técnica, essa foi como que imediata" (P3.V1.1 – P2HFF#02)
		"Inicialmente as questões de segurança não são uma prioridade. Interessa antes de mais por os protocolos a funcionar. Fazer com que haja passagem de informação entre sistemas. Posteriormente e gradualmente as questões da segurança começam a ser colocadas e implementadas" (P3.V1.1 – P2HFF#02)
		"[...] alguns conceitos na área clinica de interpretação da informação clinica e do que é a informação clinica, e quem é que tem acesso à informação clinica" (P3.V1.1 – P2HFF#03)
		"[...] a questão de facto da privacidade – quem regista e quem consulta os dados – faz com que alguns clínicos se retraiam muito, por não se sentirem muito confortáveis no entendimento que fazem desta questão" (P3.V1.1 – P2HFF#03)
		"Ainda assim internamente carecem de regras que permitam criar comunicações com uma maior fiabilidade. [...] Não conseguem ainda ser as normas a estabelecer as regras para a interoperabilidade ao nível da segurança" (P3.V1.1 – P2SPMS#03)
		"[...] é mesmo a partilha dos dados, em termo de segurança, de quem acede, e mesmo também, falando mais da parte para a qual estou mais sensibilizada, que é o volume de informação" (P3.V1.1 – P2SPMS#04)
		"Antes de se dar outro passo de gigante, deveria de alguma forma parar-se, olhar bem para a situação atual e poder identificar e corrigir riscos existente" (P3.V1.1 – P2SPMS#04)
		"Acho positivo a partilha de dados com outras organizações de saúde, desde que esteja garantida a sua segurança" (P3.V1.1 – P2HES#02)

	"As maiores preocupações de funcionarem em rede têm a ver com a segurança da informação. É importante salvaguardar os dados, tanto na componente de rede de comunicação entre instituições, como nos dados que circulam na rede e na forma como circulam na rede" (P3.V1.1 – P2HES#02)
	"Tem que haver uma confidencialidade dos dados, temos que saber quem é que acede ao quê. [...] no sentido de responsabilizar as pessoas" (P3.V1.1 – P2HES#02)
	"A segurança assim uma das maiores preocupações. E hoje em dia já estamos a pensar nos dados que estamos a passar para o exterior" (P3.V1.1 – P2HES#03)

P3.V1.2	***Perfil 1** / Responsáveis pela implementação e coordenação da PDS*	***Perfil 2** / Técnicos e responsáveis pelos sistemas de informação*
Padrão		
Colaboração		
Partilha		
Padronização		
Segurança dos dados		
Confiança		
	"Sim. [...] maior sensibilização. Uniformização [...], que sigam as mesmas regras, o que acabará sem dúvida por contribuir para a partilha de dados de uma forma mais segura" (P3.V1.2-P1ULSNA#01)	"É desejável e já acontece [...], de uma forma informal. Seria vantajoso, [...], partilhar as melhores práticas ao nível da segurança (P3.V1.2-P2ULSNA#2)
	"Sem dúvida, facilitava imenso a protecção de dados" (P3.V1.2-P1USF#01)	"Caminhar neste sentido, através de um padrão vai exigir [...], os mesmos sistemas de segurança. O utente sai beneficiado" (P3.V1.2-P2ULSNA#03)
	"É necessário uma maior interoperabilidade ao nível da segurança que suporte a partilha de experiências, promova uma padronização [...], aprender [inclusive] com as más práticas. Esta colaboração poderia fazer com que existisse um domínio de confiança mais alargado" (P3.V1.2-P1.INEM#01)	"As questões da segurança da informação terão de ser sempre colocadas" (P3.V1.2-P2USF#02)
	"São questões de interoperabilidade técnica e também organizacional. A partilha de dados entre instituições depende de uma interoperabilidade não-técnica aos níveis da segurança, da protecção de dados, protocolos de entendimento" (P3.V1.2 – P1HFF#01)	"Sim, só com a experiência de vários [organizações] é que se consegue padronizar! (P3.V1.2-P2INEM#03)
	"Não vejo desvantagens nesta partilha de soluções e colaboração. Apesar de ter um efeito quase invisível, as pessoas tendo a perceção de uma melhor segurança, as pessoas sentem-se mais confortáveis na utilização dos sistemas e na troca de informação" (P3.V1.2 – P1SPMS#02)	"Com certeza que sim. [...] somos obrigados a repensar a segurança destes dados. [...] o alinhamento de medidas de segurança. [...] maior informação sobre segurança quando se partilha dados" (P3.V1.1-P2INEM#04)
	"Neste momento as pessoas preocupam-se com a possibilidade de furto de dados na área da saúde [...]" (P3.V1.2 – P1SPMS#02)	"Absolutamente, porque se houvesse um padrão que todos tivessem que seguir, [...] seria muito melhor. Produzia-se um domínio de confiança maior. Cria-se uma confiança maior entre as instituições [...]" (P3.V1.2-P2INEM#09)
	"Eu acho que em todas as matérias que digam respeito aos sistemas de informação, às normas e às regras, deveria de haver mais colaboração entre estes profissionais. No suporte aquilo que é a privacidade dos dados, uma partilha de experiências era de todo uma mais-valia" (P3.V1.2 – P1HES#01)	"Sim é desejável uma maior colaboração. [...] uma maior colaboração, [...] tornaria mais fácil a segurança dos dados (P3.V1.2-P2INEM#10)
		"Sim é possível e muito importante" (P3.V1.2 – P2HFF#02)
		"Ajuda-nos a fazer uma melhor gestão da mudança. Se quisermos alterar para um novo sistema, a interoperabilidade não é só com outras instituições, também é interna. Se tivermos um bom plano de interoperabilidade interna, ajuda-nos na interoperabilidade com outras instituições. Vai sem dúvida ajudar no processo de gestão da mudança" (P3.V1.2 – P2HFF#02)
		"É desejável que haja aqui uma colaboração [interoperabilidade não-técnica] em assuntos como a segurança, a proteção e a privacidade de dados que suporte depois este contexto de colaboração. O objetivo é que depois a tecnologia consiga garantir o paradigma da informação e do acesso à informação" (P3.V1.2 – P2HFF#02)
		"Eu julgo que sim. Os efeitos práticos são muitos" (P3.V1.2 – P2SPMS#03)
		"É nossa preocupação que o mecanismo de comunicação e o canal de comunicação sejam seguros e que respondam a processos de segurança. Agora faltam as outras camadas, nomeadamente as aplicações" (P3.V1.2 – P2SPMS#03)
		"Sim. O CAIC (comissão de acompanhamento de informação clinica) é um bom exemplo desta colaboração. Tem vários grupos de intervenção. Partilhar experiências, entre organismos nacionais, para que a segurança de infraestruturas possa andar ao lado da segurança da informação" (P3.V1.2 – P2SPMS#04)
		"A passagem de conhecimento é sem dúvida o efeito prático mais evidente que pode resultar da colaboração entre instituições, assim como a passagem de tecnologias, processos e *standards* usados, os bons e os maus resultados" (P3.V1.2 – P2SPMS#04)
		"Deste modo muitas instituições não necessitavam de começar do zero" (P3.V1.2 – P2SPMS#04)
		"O ideal era existir uma uniformização dos sistemas de informação, com diretrizes vinda do ministério da saúde, no sentido definir prioridades de uniformização. [...] Uma maior colaboração é assim essencial a esta uniformização" (P3.V1.2 – P2HES#02)
		"A segurança informática dependeu muito da nossa formação. Fomos um bocado autodidactas. A área da segurança ainda é uma lacuna muito grande ao nível dos hospitais" (P3.V1.2 – P2HES#03)

P3.V2.1	A análise de risco é uma realidade	Qual o seu contributo para a segurança e a privacidade dos dados
Padrão Risco Infraestruturas Segurança Disponibilidade	"Houve apenas um projeto desenhado em equipa, documentado, para a segurança física da infraestrutura interna [...]. Foram definidos os riscos e pessoas autorizadas" (P3.V2.1-P2ULSNA#02)	Apresenta como vantagem o facto de podermos ser mais concisos" (P3.V2.1-P2ULSNA#03
	"De certa forma sim, somos cuidadosos em relação aos riscos" (P3.V2.1-P2ULSNA#03).	"Se orientarmos esta análise apenas à infraestrutura e não tendo em conta a informação, as aplicações não vão funcionar da mesma forma" (P3.V2.1-P2USF#02
	"As políticas de protecção de dados devem ser sempre desenvolvidas com base naquilo que é a análise do risco" (P3.V2.1-P2USF#02)	"Grande parte da estrutura está assente em empresas externas [...], mas isto não impede que haja uma análise do risco. Devemos caminhar para no futuro dar mais atenção a este requisito, à análise de risco, de preferência que pudesse evoluir para a protecção de dados" (P3.V2.1-P2INEM#03)
	"A análise do risco realizada é orientada à infraestrutura e à informação" (P3.V2.1-P2USF#02)	"As coisas [em segurança] têm sido feitas mais pelo senso comum. [...] uma análise de risco poderia contribuir para um desenvolvimento mais integrado dos sistemas quanto à segurança" (P3.V2.1-P2INEM#04)
	"A Privacidade dos dados deve ser encarada com uma questão de risco. Apesar de ainda não ser uma realidade, estas questões devem gradualmente ser integradas na análise do risco" (P3.V2.1-P2USF#02)	"Sabe-se que determinadas pessoas que pertencem a um determinado grupo ou serviço podem aceder a determinado tipo de dados". "Deveria haver uma análise de risco prévia para a segurança como um todo. Há medidas que foram tomadas, mas que foram sendo desenvolvidas à medida que foram surgindo as necessidades (numa adaptação contínua), e não através de um processo de raiz que identifica-se os riscos.". "Houve numa primeira fase a preocupação de salvaguardar acessos físicos, sistemas redundantes" (P3.V2.1-P2INEM#09)
	"É necessário uma infraestrutura bem instalada, para poder posteriormente dar maior atenção à questão dos dados". "[...] ainda vamos demorar algum tempo a chegar à camada de proteção e dados a sério" (P3.V2.1-P2USF#02)	"A segurança é apenas uma preocupação de quem desenvolve as soluções. Só que toda a segurança deveria nascer numa análise rigorosa do risco e deveria ser bem planeada" " (P3.V2.1-P2INEM#10)
	Não, não foram baseadas numa análise de risco" (P3.V2.1 – P2INEM#09)	"A nossa maior preocupação é a disponibilidade e qualidade da informação. Não nos preocupamos muito com a segurança dos dados, porque muitas vezes acaba por ser um "empecilho" ao início dos sistemas. O que interessa é colocar os sistemas a funcionar. Não deveria ser assim" (P3.V2.1 – P2HFF#02)
	Não no nosso caso" (P3.V2.1 – P2INEM#10)	"As políticas de segurança são do tipo reactivo e não proactivo. Agora é desejável que exista uma análise do risco que suporte as medidas de segurança, e que depois possam ser harmonizadas com outras organizações" (P3.V2.1 – P2HFF#02)
	"Não, mas temos uma ideia dos riscos existentes e das vulnerabilidades. Mas não existe um documento formal. Reagimos perante uma situação e damos origem a algumas regras" (P3.V2.1 – P2HFF#02)	[...] o 1º passo para a privacidade do nosso ponto de vista está em garantir a estrutura de dados. Se eu não tenho informação estruturada eu não posso garantir privacidade. É o tudo ou nada. 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)
	"A análise de risco deve ser preponderante a estas matérias. Mas nós não a exercemos. Em termos de maturidade o hospital ainda não está aí [na análise do risco]" (P3.V2.1 – P2HFF#03)	"Fazer uma análise do risco sobre qualquer sistema é fundamental, porque conhece-se as vulnerabilidades, consegue-se caracterizar o risco, e procurar-se resolver o risco. E isto numa situação em que o risco acontece é fundamental ter os caminhos traçados e pensados, e perceber qual é o real impacto do risco" (P3.V2.1 – P2SPMS#03)
	"Agora esta decisão de negócio de que forma a que impacta em termos de risco isso é praticamente, não digo tabu, mas está muito longe da atenção dos actores. Sem dúvida que é um caminho a percorrer" (P3.V2.1 – P2HFF#03)	"Faz todo o sentido que esta questão da privacidade dos dados também tenha por base uma análise de risco. A privacidade e proteção são um risco, não na vertente organizacional, não na vertente financeira, mas diria que na perspetiva do cidadão, representa um risco" (P3.V2.1 – P2SPMS#03)
	"[...] nós estávamos a zeros neste domínio. Nós e os outros hospitais, a maioria. Uma das razões é porque não havia informação para proteger, ou seja, existia em papel os procedimentos tradicionais. Quando iniciamos a informatização, este primeiro passo foi demasiado imaturo" (P3.V2.1 – P2HFF#03)	"Se os projetos, no desenho tecnológico, *à priori*, fizessem um impacto de privacidade, uma análise de impacto sobre a privacidade, [...] provavelmente minimizavam o risco" (P3.V2.1 – P2SPMS#03)
	"Ainda não é uma prática comum o desenvolvimento de práticas de segurança com base numa análise de risco, mas deveria ser uma realidade de construir com base no risco" (P3.V2.1 – P2SPMS#03)	"Esta questão da privacidade deveria ser tratada como um risco, faz todo o sentido, ser tratada como um risco. Os dados hoje em dia são um risco muito grande" (P3.V2.1 – P2SPMS#04)
	"Os procedimentos de segurança não nasceram numa análise de risco. Surgem do nosso conhecimento, com base naquilo que são alguns padrões de segurança e que têm que ser implementados. As	"Uma análise de risco poderia ser uma ferramenta excelente, embora nós já sabemos quais são os riscos. Temos que fazer uma análise de risco que em simultâneo inclua as infraestruturas e a organização, e os dados. Até porque já temos algumas medidas implementadas, esta seria uma ferramenta integradora" (P3.V2.1 – P2HES#02)

	políticas que são implementadas estão de acordo com estes padrões" (P3.V2.1 – P2HES#02)	"Seria vantajoso trabalhar com ferramentas de análise do risco e depois definir medidas de proteção e segurança. Gradualmente incluir a privacidade. Para conhecermos onde temos falhas, temos que primeiro identificar estas falhas, e depois procurar resolve-as" (P3.V2.1 – P2HES#03)
	"A análise de risco não o é a 100%. Existe o conceito, é utilizado. O Conhecimento não é o suficiente, é necessário mais conhecimento [em análise do risco]" (P3.V2.1 – P2HES#03)	"É uma área de colaboração com outras instituições, uma vez que o risco é muito parecido" (P3.V2.1 – P2HES#03)

P3.V3.1 *Perfil 2 / Técnicos e responsáveis pelos sistemas de informação*

Padrão encontrado	**Importância e situação atual**	**Evolução desejável**
Autenticação	"[…] a identidade digital é importante para o futuro da partilha de dados" (P3.V3.1-P2ULSNA#02)	"Nem todas as aplicações têm a segurança que deveriam ter neste domínio". "[…] deveria haver uma preocupação em desenvolver uma autenticação única para todas as aplicações." "[…] a autenticação evoluiu, prevendo-se a autenticação via cartão de cidadão ou cartão da ordem dos médicos. Penso que o cartão do cidadão não deveria ser utilizado apenas neste ato de autenticação, mas ser utilizado no acesso a qualquer aplicação. Seria uma forma única de identificar o individuo, universalmente e de uma forma segura." (P3.V3.1-P2ULSNA#02)
Sistema único	"[…] a uniformização de processos ou sistemas, para que em termos de comunicação a interoperabilidade não seja tão complicada". (P3.V3.1-P2ULSNA#03)	**"**O ideal é que todos estes sistemas evoluíssem para um sistema único, centralizado. Apesar dos problemas de segurança estamos a caminhar para que os sistemas de autenticação confiem uns nos outros." (P3.V3.1-P2ULSNA#03)
Interoperabilidade	"Pode não ser completamente preponderante. É um dado a ter em conta. […] Não faz sentido a duplicação de dados existente na atualidade." (P3.V3.1-P2USF#02)	"[…] estes deveriam evoluir, com toda a certeza, com que o conseguíssemos fazer com base num único local. A existência de múltiplos sistemas de autenticação dificulta inclusive a mobilidade de profissionais. Deveria haver uma maior interoperabilidade entre estes sistemas. Não faz sentido, haver um identificador para a saúde, outro para a finanças e assim sucessivamente." (P3.V3.1-P2USF#02)
	"É preocupante quando um profissional de saúde, por exemplo, num sistema tem umas credenciais de autenticação e num outro sistema apresenta credenciais diferentes." "Vamos pensar que se todos tiverem sempre a mesma identificação, com base num sistema único e centralizado, a questão da interoperabilidade seria facilitada certamente, porque estávamos a trabalhar todos sobre o mesmo contexto e não contextos diferentes que obrigatoriamente depois têm de se relacionar entre si. Não chega partilhar dados, é necessário também partilhar a identidade digital, a camada de autenticação. (P3.V3.1-P2INEM#03)	"Se as instituições estão a partilhar dados deverão evoluir para um sistema unificado de identidade." (P3.V3.1-P2INEM#03)
	"Havendo um único sistema que gere a identidade digital de todos os profissionais, estamos a caminhar para um ambiente mais seguro […]" (P3.V3.1-P2INEM#04)	"Era desejável que estes sistemas evoluíssem para um sistema único ou que pelo menos comunicassem uns com os outros". (P3.V3.1-P2INEM#04)
	"Hoje em dia não se consegue "sobreviver" sem uma identidade digital." (P3.V3.1-P2INEM#09)	"[…] a identidade digital deveria ser tratada de um outra forma. A autenticação da pessoa, não deve servir apenas para autenticar a pessoas, mas também para a poder responsabilizar pelo que fez durante o dia. Isto por questões de segurança. Faz sentido, evoluir-se para um sistema único dos utilizadores, que permita abranger todas as organizações." (P3.V3.1-P2INEM#09)
	"Quanta mais vezes eu tiver que me autenticar, […], maior vai ser o risco de segurança, […]" (P3.V3.1-P2INEM#10)	"Deveria evoluir-se para um sistema o mais único possível, em que a minha autenticação seja comum a todos os sistemas. Seria no fundo um nível tecnológico de suporte a um domínio mais seguro, para partilha de dados." (P3.V3.1-P2INEM#10)
	"Veja-se o caso dos estagiários que se movimentam entre os vários hospitais, em que é difícil fazer a gestão da sua identidade digital" (P3.V3.1 – P2HFF#02)	"[…] deveria começar por haver um sistema de autenticação central. […] O que defendo é no futuro haver também uma interoperabilidade entre estes sistemas a nível nacional. É o conceito de federação" (P3.V3.1 – P2HFF#02)
	"É necessário garantir uma identidade digital uniforme em todo o sistema de informação" (P3.V3.1 – P2HFF#03)	"[…] é necessário federar a identidade digital. Se o profissional de saúde trabalha em mais de uma instituição, e cada vez este potencial vai ser maior, para mim a identidade digital no SNS deveria ser única e era cedida pela ordem em ligação com o sistema central" (P3.V3.1 – P2HFF#03)
	"Ou seja, se quisermos ter uma visão agregada é difícil. Isto porque nós só controlamos o interior do nosso sistema. É possível saber aquilo que temos dentro mas temos muita dificuldade sem saber quando os dados saem para fora, ou quando temos que adotar um sistema externo, e depender dele " (P3.V3.1 – P2HFF#03)	"Os modelos em si podem ser distribuídos, centrais, federados. Face a nossa dimensão nacional, acredito que é possível ter um modelo centralizado, ainda que depois possa fornecer serviços a outras aplicações ou sistemas locais" (P3.V3.1 – P2SPMS#03)
	"A identidade digital é a nossa base de subsistência. Conheço bem a dificuldade que é, e que tem sido no nosso universo conseguir caracterizar os nossos utilizadores com alguma qualidade" (P3.V3.1 – P2SPMS#03)	"O modelo de gestão para a identidade que eu defendo, acaba por identificar o utilizador final muito com base naquilo que é a sua origem. Já o fizemos no processo das vinhetas, para os médicos, em que foi desenhado um processo em conjunto com a ordem dos médicos, que permitiu cruzar dados entre três entidades, para conseguirmos ter a certeza que num processo de registo, que a pessoa que se está a autenticar, do ponto de vista eletrónico é quem diz ser" (P3.V3.1 – P2SPMS#03)
	"Um dos problemas é que temos autenticações muito diversas" (P3.V3.1 – P2SPMS#04)	"Os entraves ao desenvolvimento de sistemas de identidade conjuntos são mais organizacionais do que tecnológicos" (P3.V3.1 – P2SPMS#03)
	"A mudança de sistemas não deveria obrigar a uma nova autenticação mas apenas à validação da autenticação anterior.	"Face à heterogeneidade dos sistemas, deveria evoluir-se para uma autenticação igual, um sistema único, e uma única autenticação ser o suficiente para utilizar várias aplicações, mesmo que noutra

	Cada vez mais temos profissionais em mobilidade hospitalar [...]" (P3.V3.1 – P2SPMS#04)	instituição" (P3.V3.1 – P2SPMS#04)
	"Isto hoje é uma malha de instituições" (P3.V3.1 – P2HES#02)	"Para além de uma uniformização de um sistema de autenticação, temos que ter uma política de autenticação forte" (P3.V3.1 – P2HES#02)
	"Algumas tecnologias, aplicações, ainda não permitem a partilha de dados de identidade digital e autenticação. Cada uma tem as suas regras de autenticação" (P3.V3.1 – P2HES#03)	"Deveriam também estes sistemas muito heterógenos falar entre si. [...] Caminhar-se para um sistema único a nível nacional que autentica-se os profissionais" (P3.V3.1 – P2HES#02)
		"É possível uniformizar os métodos de autenticação, com base em dados dos médicos centralizados, neste caso na SPMS. [...] O caminho é um sistema centralizado de autenticação" (P3.V3.1 – P2HES#03)

P3.V4.1	***Perfil 2** / Técnicos e responsáveis pelos sistemas de informação*
Padrão encontrado Garantias Medidas específicas Regras específicas Risco Pouco conhecimento e experiência	[…] a utilização primária é aquela que pode envolver mais riscos." (P3.V4.1-P2ULSNA#02)
	[…] penso que o foco principal de preocupações é a utilização primária." (P3.V4.1-P2ULSNA#03)
	"Os cenários de utilização secundária são cada vez mais comuns, mais preocupantes. Não acredito é que as instituições estejam a pensar nestes e a adotar medidas eficazes de proteção de dados. É ao nível do ministério (através de alguém especializado em privacidade) que faz sentido que estas questões sejam analisadas de uma forma transversal para todas as instituições, para que todos trabalhem da mesma forma. (P3.V4.1-P2USF#03)
	"Apesar de nosso caso a utilização primária ser mais preocupante que a utilização secundária, tem que haver soluções, garantias para a utilização secundária, garantias que permitam, que tal como na primária, os dados não são violados." (P3.V4.1-P2INEM#03)
	"Tudo depende dos contextos. Mas a segunda hipótese poderá ser aquela, que mais problemas poderá levantar. Tudo depende da natureza da própria informação. Deveriam ser pensadas medidas especificas para estes cenários, pois o prejuízo de uma má protecção será maior do que na utilização primária." "Há que repensar todas as utilizações secundárias – tenho a ideia de que alguém que tenha que ter, que de acordo com a sua função, tenha que aceder a um conjunto de dados, está por inerência afeto a um dever de confidencialidade sobre aquela informação." "[…] a minha preocupação prende-se com a utilização indevida de determina informação ou precavermo-nos que determinadas pessoas possam, por não ter suficiente conhecimento sobre a utilização de um determinado conjunto de dados, destrui-los inadvertidamente. E aqui a protecção de dados fica em causa." (P3.V4.1-P2INEM#04)
	"[…] os principais problemas estão associados à utilização primária dos dados. Para a utilização secundária deveriam existir também regras bem definidas, […]. Existe sempre um risco quando alguém está interessado em recolher estes dados, para diversos fins. Não se conhece muito bem a utilização secundária dos dados no domínio da saúde. A partir do momento em que os dados saem da organização, pode acontecer tudo." (P3.V4.1-P2INEM#09)
	"[…] os maiores problemas surgem na utilização primária, que estão associados principalmente aos problemas de utilização das tecnologias de informação. Normalmente quem faz utilização secundária dos dados tem a preocupação de preservar a identidade dos dados. Existe a este nível uma maior proteção. Quem faz isto tem o cuidado de preservar a privacidade. Elimina todos os fatores que possam colocar em causa a privacidade. Isto não elimina a necessidade de haver regras próprias para a utilização secundária. Até porque é preciso avaliar que tipo de utilização se vai fazer com os dados." (P3.V4.1-P2INEM#10)
	"Os maiores problemas de privacidade penso surgirem na utilização primária" (P3.V4.1 – P2HFF#02)
	"Dependendo do objetivo da utilização secundária dos dados, também deveria existir normas para a utilização dos dados. É importante identificar o individuo que vai utilizar estes dados, o seu objetivo e os riscos associados. Tem que se ajustar a proteção com aquilo que é o objetivo da utilização [secundária] dos dados" (P3.V4.1 – P2HFF#02)
	"Existe um certo facilitismo, apesar das medidas que têm sido tomadas" (P3.V4.1 – P2HFF#02)
	"Temos muitos problemas com a utilização secundária, e é um assunto que está a ser discutido neste momento. Há um procedimento que vai ser agora desenhado […] porque a DGTI levantou aqui a legitimidade da extração de dados fora de qualquer perfil de acesso" (P3.V4.1 – P2HFF#03)
	"Tem que existir uma única fonte de saída de informação, para que esta seja fornecida corretamente, contextualizada e para o fim a que se destina. E também para garantir a proteção da propriedade da informação e que a informação é utilizada apenas para aquele fim" (P3.V4.1 – P2HFF#03)
	"A questão tal como está, ainda está muito imatura. Ou seja, corremos muitos riscos. Podemos estar a dar informação a mais, não digo por negligência, mas por descuido, por desconhecimento" (P3.V4.1 – P2HFF#03)
	"O facto de nós estarmos cada vez mais a partilhar dados em ambiente alargado pode vir a agravar-se aquilo que é a utilização secundária de dados" (P3.V4.1 – P2HFF#03)
	"Eu diria que podemos ter mais problemas talvez na utilização secundária. Incluindo aqui os processos de integração. Muitas vezes os sistemas são desenhados com um determinado objetivo, e depois aparecem um conjunto de integrações e também interoperabilidade à volta, que fogem do processo inicial" (P3.V4.1 – P2SPMS#03)
	"A utilização secundária pode ser mais preocupante. No nosso caso, nós disponibilizamos muitos dados a várias entidades para estatísticas, e são enviados todos os dados registados, existindo alguns cuidados com dados identificados" (P3.V4.1 – P2SPMS#04)
	"Deveria haver um maior controlo sobre todos estes processos, uma vez que estes processos têm tendência a crescer muito" (P3.V4.1 – P2SPMS#04)
	"A utilização secundária preocupa mais no sentido em que alguém, que eventualmente, não deveria ter acesso a esses dados, conseguiu aceder-lhe" (P3.V4.1 – P2HES#02)
	"É necessário ter algum cuidado com estas pessoas, com os fins da utilização dos dados. É aqui que no meu ponto de vista poderão surgir mais fugas de informação" (P3.V4.1 – P2HES#02)
	"Agora sempre que se extraírem dados tem que haver a aplicação de um conjunto de medidas de proteção, para garantir que o utente entra na estatística mas não se sabe quem é" (P3.V4.1 – P2HES#03)

P3.V5.1	***Perfil 2** / Técnicos e responsáveis pelos sistemas de informação*
Padrão encontrado Necessário Incluir os dados	"Trabalha-se muito na segurança física de dados, em planos de contingência para links primários, links de backup de dados, mas nada focado na privacidade dos dados." "Mas tem que se começar a caminhar neste sentido." (P3.V5.1-P2ULSNA#02)
	"Sim, digamos que ao nível local é possível." "É conteúdo, tal como para a segurança, desejável haver planos de contingência para que se possa agir rapidamente se foi detetado a utilização indevida de dados. " (P3.V5.1-P2ULSNA#03)
	"Acho que sim, deveríamos estar-nos a posicionar ao nível dos dados." "Se as instituições ainda não pensaram nisto deveriam pensar, faz todo o sentido." (P3.V5.1-P2USF#02)
	"Sim deveríamos também pensar em planos de contingência para os dados." "[…] tem que haver sempre alguns planos de contingência, a garantia que se algo correr mal, se consiga recuperar ou reconstituir aquilo que tínhamos. Apenas backups de bases de dados. Não é nitidamente suficiente. É necessário pensar mais à frente." (P3.V5.1-P2INEM#03)
	"Eu penso que sim, os dados são, digamos o valor mais precioso que existe em qualquer organização ou em qualquer sistema." "Por enquanto ainda estamos ao nível da disponibilidade dos sistemas. Ainda não estamos ao nível de situações de quebra de confidencialidade dos dados. Vamos ter que caminhar neste sentido." "Mas se houver uma quebra de confidencialidade num conjunto de dados os sistemas ainda não conseguem detectar esta quebra. Concordo que se deverá caminhar no sentido de se perceber a existência de quebras de confidencialidade e poder agir rapidamente, minimizando os possíveis impactos." (P3.V5.1-P2INEM#04)
	"Possível é!" "Se se conseguir identificar uma pessoa com base nestes dados é possível prever algumas medidas de proteção para estas situações." (P3.V5.1-P2INEM#09)
	"Desejável é sempre. Não me parece é que depois haja muita solução. Principalmente no caso de haver perda de dados. É desejável que haja nestas situações um plano de contingência no sentido de minimizar o impacto causado. Se houver uma fuga ou adulteração de dados têm que ser pensadas mediadas, que permitam proteger os visados. […] Tem que haver medidas adaptadas a cada uma das realidades, a cada contexto." (P3.V5.1-P2INEM#09)
	"Já desenvolvemos um plano de contingência, […] Só que não existe grande proteção ao nível dos dados. Deveríamos estar a caminhar para o nível dos dados" (P3.V5.1 – P2HFF#02)
	"Deveríamos ter um plano de contingência no caso da perda de dados" (P3.V5.1 – P2HFF#02)
	"Havendo um furto de informação deveríamos ter um plano de contingência. […] Estes planos devem estar associados à identificação do risco que corremos e de alguma forma definir algumas tarefas que anulem este risco" (P3.V5.1 – P2HFF#02)
	"Nós só agora, é que o hospital atingiu a maturidade para se preocupar com o plano de contingência para a falência do sistema de informação" (P3.V5.1 – P2HFF#03)
	"Agora o risco está a aumentar exponencialmente à medida que a qualidade de informação tem mais valor" (P3.V5.1 – P2HFF#03)
	"Nós neste momento não temos instrumentos que nos permitam aferir de situações de dados adulterados, roubo de dados. Temos a auditoria clinica que é feita apenas à qualidade dos dados – saber se o campo foi bem preenchido, se o diagnóstico faz sentido" (P3.V5.1 – P2HFF#03)
	"Sim é possível. Sempre que existem falhas de segurança, que impliquem estar em causa os dados, isto é a proteção de dados, obriga a notificar os donos desses dados" (P3.V5.1 – P2SPMS#03)
	"Existem alguns mecanismos previstos para estas situações, […] Mas do ponto de vista de segurança, não da informação" (P3.V5.1 – P2SPMS#03)
	"Para situações de furto de informação sobre grupos de risco, deveria haver planos de contingência. Deveria saber-se o que desenvolver no imediato" (P3.V5.1 – P2SPMS#04)
	"Perante uma situação de violação e furto de dados, claro que sim, devemos ter um plano de contingência aplicado aos dados" (P3.V5.1 – P2HES#02)
	"Deveriam existir mecanismos que permitissem detetar este tipo de violação. Não sei se uma monitorização, se auditorias frequentes aos sistemas de informação. Tem que se ter sistemas que suportem este tipo de deteção e depois atuar" (P3.V5.1 – P2HES#02)
	"Sim faz todo o sentido pensar-se em planos de contingência. Se os dados forem roubados convém haver um mecanismo para que eles não consigam ser vistos, nomeadamente através da sua encriptação" (P3.V5.1 – P2HES#03)

3. Data Display

P3	Matriz de análise da opinião sobre P3. Segurança e infraestruturas		
Variáveis dependentes	*Padrão encontrado*	*Contexto/desempenho e evolução necessária*	*Relação com a privacidade dos dados*
P3.v1. A segurança de infraestruturas locais e de comunicação, a sua interoperabilidade técnica e não-técnica (a "estandardização/padronização das melhores práticas de segurança" específicas de cada sistema são essenciais ao desenvolvimento de uma plataforma segura e de confiança), são preponderantes para camadas superiores de segurança, nomeadamente a privacidade dos dados.	Colaboração/partilha Padrão/padronização Confiança Disponibilidade dos sistemas	A segurança ainda é uma lacuna. Atualmente focada apenas na disponibilidade dos sistemas. Maior interoperabilidade [não técnica] ao nível da segurança. Alinhamento de medidas de segurança. Evolução da segurança para a proteção de dados. Maior sensibilidade em relação à privacidade dos dados. Estabelecer regras de interoperabilidade. Identificar os riscos existentes. Um bom plano de interoperabilidade interna, ajuda na interoperabilidade com outras instituições. Uniformização dos SI.	Rastreabilidade dos dados. Controlo do acesso e segurança da informação. Domínio de confiança mais alargado entre organizações. Partilha de experiências, padronização das melhores práticas. Garantia de confidencialidade. A partilha de dados entre instituições depende de uma interoperabilidade não-técnica aos níveis da segurança, da proteção de dados, protocolos de entendimento.
P3.v2. Uma análise de risco em segurança e uma análise do impacto sobre a privacidade (PIA), que englobem todos os equipamentos e situações de recolha, armazenamento, utilização e partilha de dados, são dois instrumentos decisivos para o enquadramento e conhecimento das situações problemáticas à privacidade dos dados.	Risco Infraestruturas Segurança Disponibilidade	É necessário uma análise prévia do risco para a segurança. É necessário promover colaboração no conhecimento do risco. As medidas de segurança surgem de alguns *standards* e da experiência acumulada. A disponibilidade dos sistemas ainda é uma prioridade o que contribui para que a análise do risco se limite às infraestruturas. A análise do risco não é ainda uma prática ao nível dos SI - evolução da análise do risco para o nível da privacidade dos dados.	Os dados hoje em dia são um risco muito grande. Privacidade dos dados como uma questão de risco. Uma análise de impacto sobre a privacidade minimiza o risco - reconhecimento das vulnerabilidades e do impacto do risco. Análise do risco no suporte à proteção dos dados. Suporte ao desenvolvimento integrado da segurança. Análise do risco como ferramenta integradora de medidas de proteção e segurança.
P3.v3. No domínio da segurança e infraestruturas, a identidade digital, os sistemas de gestão de identidade, e a confiança (federação) e interoperabilidade entre estes sistemas, são um componente essencial à gestão e monitorização da confidencialidade e privacidade dos dados.	Autenticação Sistema único Interoperabilidade	Uniformização de processos ou sistemas. Partilha da identidade digital, dos mecanismos de autenticação. Forma única de autenticação. Confiança entre sistemas de identidade digital no suporte à mobilidade de profissionais. Uniformização das regras de autenticação. Federação dos sistemas de identidade digital.	Uniformização do conceito de identidade digital. Responsabilização. Mais segurança na partilha de dados.
P3.v4. A segurança em cenários de exposição de dados a ambientes vulneráveis de "não-produção" é essencial a preservação da sua privacidade. Os requisitos de privacidade dos dados nestes contextos devem cumprir com os requisitos legais.	Garantias Medidas específicas Regras específicas Risco Pouco conhecimento e experiência	A utilização secundária no geral é mais preocupante. Situações funcionam sem o suporte de proteção exigível. Necessidade de repensar situações, tipos e contextos de utilização dos dados. É necessário conhecer o risco associado. Definição de regras e medidas específicas e transversais – em colaboração com outras organizações.	Contextos propícios à utilização indevida dos dados, por falta de conhecimento. Dever de confidencialidade Necessidade de preservar a identidade dos dados. Necessidade de ajustar o nível de proteção com aquilo que é o objetivo da utilização dos dados, e a natureza dos dados.
P3.v5. A existência de um plano de contingência para lidar com os efeitos de eventos não previstos como a perda acidental, destruição ou deterioração de dados pessoais, e tratamentos ilegais e não autorizados, contribui para anular possíveis quebras de privacidades destes dados.	Necessário Incluir os dados	Desenhados apenas ao nível da disponibilidade dos sistemas. Incluir infraestruturas físicas (disponibilidade dos sistemas) e evoluir de forma a incluir os dados. Medidas adaptáveis ao contexto. Devem estar associados à identificação do risco. Necessário desenvolver mecanismos de identificação da utilização indevida dos dados.	Reposição da confidencialidade dos dados. Minimização dos impactos sobre a privacidade dos dados e sobre as pessoas afetadas (visadas). O risco aumenta com o valor e a qualidade dos dados.