Análise dos dados – P5. *Accountability*: responsabilidade e conformidade

1. Dados das entrevistas

Variável dependente – Participante

P5.V1.1

P5.V1.1 – P1ULSNA#01	Poder pode, mas é um caminho complicado de seguir. Tem tudo a ver com uma questão cultural. Quando falamos de privacidade de dados em saúde estamos a falar de dados sensíveis. Este é um processo que deve partir sempre da própria tutela, envolvendo todos os profissionais, numa equipa multidisciplinar, e de diversas instituições. A elaboração de políticas de privacidade com base na experiência de múltiplos locais facilita que a mensagem chegue a todos os envolvidos.
P5.V1.1 – P2ULSNA#02	Se for feito a nível local não, se for feito a nível nacional penso que sim. Isto deve-se ao facto de maior parte das aplicações não ser desenvolvidas por nós e em algumas situações controladas por nós. Apesar de os dados estarem dentro da nossa organização, a construção do acesso a estes dados não é desenvolvida por nós. De iniciativa local podemos estar a criar uma intenção e depois não a conseguimos manter com qualidade. Existem situações onde o fabricante da aplicação não permite o acesso direto à base de dados. Um programa de responsabilidade tem que ser muito abrangente, para todas as organizações, devendo abranger conselhos de administração, conselhos de ética, sendo que estas questões ficam muito aquém dos conhecimentos que as comissões de ética possuem. Estamos a falar de três grupos: administração, área clinica, e tecnologias de informação.
P5.V1.1 – P2ULSNA#03	Pode contribuir, aliás contribuí. A elaboração deste programa, atendendo à estrutura da saúde tem que ser organizado a nível superior, nomeadamente pela SPMS. Vejo este programa de responsabilidade mais ao nível da colaboração do que ao nível da unidade local de saúde. Internamente um processo destes deve iniciar-se na administração, como é óbvio, e a incluir a parte dos sistemas de informação.
P5.V1.1 – P4ULSNA#06	Esta questão entronca no princípio da confidencialidade que falei na questão anterior. Penso que esta questão será necessariamente diferente no sistema público e no sistema privado. Penso que no privado será mais acutilante um programa de responsabilidade, porque muitas vezes as pessoas podem-se deixar levar pela estratégia comercial e esquecer eventualmente questões que salvaguardem a segurança e a confidencialidade dos dados. No público existe à partida uma cultura de respeito, ainda antes do surgimento dos sistemas tecnológicos. Se conseguirmos identificar que alguém violou o princípio da confidencialidade, qualquer que seja o seu nível, ligado direta ou indiretamente à prestação de cuidados de saúde, ou apenas da parte administrativa, existe responsabilidade disciplinar. No fundo o que estamos a fazer hoje é transpor estes dados, já guardados em processos clínicos em ficheiros de papel, para os novos sistemas de informação que até podem partilhar os dados com outras instituições. Existem já mecanismos que garantem a segurança, a confidencialidade, a eficácia de sistema que atualmente utilizamos na prestação de cuidados. As pessoas têm conhecimento do princípio da confidencialidade e do sigilo profissional. Não podemos instituir as coisas sem

	efeito prático. Temo que nestas questões se possa avançar apenas para dar resposta a uma solicitação. Eu acho que há mecanismos, podendo não estar correto, que permitem salvaguardar a segurança, a confidencialidade, a eficácia de sistemas que atualmente utilizamos para no suporte à prestação de cuidados. Agora é necessário demonstrar que efetivamente esta ferramenta é essencial. No nosso caso, qualquer situação relacionada com pedidos de utilização de informação é sempre avaliado pelo gabinete jurídico. Se este levantar questões relativamente à violação de algum princípio de proteção de dados, informação o conselho de administração, e este atua neste sentido, de proteção dos dados. Agora, existe aqui uma questão que é muito importante, que é a tutela - Ministério da Saúde, Administração Regional de Saúde. Esta pode definir esta ferramenta, dado que estão em causa múltiplas organizações. Tem que ser alguém que tenha a visão global destas questões, que apresente um poder efetivo. A tutela é muitas vezes a primeira a solicitar informação, a qual nós enviamos de forma anónima.
P5.V1.1 – P1USF#01	Hoje em dia não existe nas instituições esta atitude de responsabilidade. Isto depende essencialmente da cultura das pessoas, e de saberem da responsabilidade dos lugares, que ocupam na sociedade. Estas regras ou responsabilização que fala poderia ser útil, mas poderá não ser decisiva. É mais uma questão de cultura, de metalizar as pessoas. Infelizmente, como em tudo, a responsabilidade, a cultura e tudo mais é ultrapassado por qualquer coisa extra que convença as pessoas a mudar de ideias. Um processo desta natureza deve iniciar sempre na tutela, sempre o ministério da saúde a definir quais são as regras, as obrigações, os direitos. A partir daqui deve ser implementado junto dos profissionais responsáveis. Não deve ser implementado no sentido de "leiam e comecem a aplicar". Já estive envolvido em algumas iniciativas muito boas do ministério da saúde, que só foram possíveis porque andamos no "terreno", junto dos profissionais, a explicar-lhes o porquê de determinado processo.
P5.V1.1 – P2USF#02	Poderia. Acho que faz todo o sentido este princípio. As normas são para cumprir. Temos que perceber sem dúvida, qual a nossa responsabilidade e por em prática medidas corretas.
P5.V1.1 – P4USF#05	Sim, vindo de cima, que obrigue a que certos itens sejam privados. A administração central deve desenvolver este princípio, uma vez é quem desenvolve todos os programas. E dentro de cada centro de saúde existir alguém responsável por isto. Têm que vir de cima, que depois sejam implementadas no local. O objetivo é que o doente não seja exposto. Estamos também a demonstrar ao doente que somos responsáveis pelo tratamento dos seus dados.
P5.V1.1 – P1INEM#01	Nitidamente sim. Este terá que ser o caminho. Apesar de se pensar que é uma responsabilidade da equipa de IT, e ao contrário do que as pessoas pensam, temos muitos dados mas não sabemos o que lá está, em que consistem, pois os utilizadores finais é que conseguem ler esta informação. Nós não temos a sensibilidade necessária para decidir se esta pessoa deveria ter acesso ou não a esta informação - isto passa pela gestão. Um programa destes poderia apresentar as principais diretrizes, que mais parte, poderiam ser materializadas em medidas e políticas de privacidade. O principal *sponsor*, digamos que deveria ser a direção, e depois claro delegar depois em outros responsáveis, até para que a política fosse efetivamente tida como um objetivo estratégico da organização.

	Para o contexto de partilha de dados com outras instituições, o ministério da saúde, à semelhança de outros projetos, é fundamental para se integrar esta visão, pois tem uma facilidade, um organismo – a SPMS, ACSS – que pode ajudar a definir políticas gerais para toda a administração pública dentro da área da saúde, e que depois de alguma forma fossem adaptados à especificidade e contexto de cada organização. Mas isto sempre integrado com aquilo que é o contexto de colaboração. Assim até o próprio ministério, saberia de uma forma transversal quais os princípios a serem aplicados.
P5.V1.1 – P2INEM#03	Tem que ser por aqui. O que infelizmente se vê na maior parte dos sítios não é uma pro-atividade, mas sim uma reação por imposição. Só quando são impostas regras é que se atua – se tem que ser vamos cumprir. Se conseguirmos alterar este paradigma seria vantajoso. Uma atitude destas tem que nascer, numa entidade reconhecida. Mas se ao nível da gestão de topo existir sensibilidade para tal, internamente numa organização, consegue-se ativar este princípio. Havendo diretrizes a este nível começa a adaptar-se todos os processos que existem, de modo a fazer cumprir estas ordens.
P5.V1.1 – P2INEM#04	Pode ser um mecanismo útil, claro que sim. Um processo destes teria de ser iniciado por um conjunto alargado de pessoas ligadas a diferentes atividades, em que nós (técnicos) estaríamos envolvidos. OS técnicos e responsáveis pelos sistemas terão aqui uma responsabilidade de desenho e implementação das soluções. Tem que haver uma consciência maior por parte dos gestores, e não só, para darem os primeiros passos. Pode ser complicado em serem os gestores a tomarem a iniciativa, dado que a sua atividade em cada organismo é algo efémera. Um departamento de planeamento por exemplo, permitiria desenvolver esta questão de uma forma mais continua. Ou então um departamento de sistemas de informação com alguém a tratar especificamente de matérias desta natureza. Tem que ser uma iniciativa conjunta de todas as organizações para dar resultado. Senão pode vir a ser um esforço inglório.
P5.V1.1 – P2INEM#09	Para haver proteção de dados, é necessário conhecer que dados vamos recolher, a sua utilidade. Tem que haver um standard que diga que dados vamos recolher. Deveria haver uma atitude proactiva em matérias de proteção de dados. As organizações são mais proactivas em questões de segurança. No nosso caso o facto de estarmos a avançar para uma certificação ISO cria esta atitude proactiva. Não podemos esperar que as coisas aconteçam para depois a seguir remediar. Uma coisa é falar em teoria, outra coisa é a prática de proteção. Agora as normas ISO são importantes, mas a definição de objetivos é ainda mais importante. Cada sistema é um sistema. Têm as suas características técnicas. Alguns componentes da norma podem não se aplicar.
P5.V1.1 – P2INEM#10	Eu acho que sim. Nós temos, não sendo das melhores, algumas medidas ativas, quanto mais não seja para defesa interna dos funcionários e dos próprios utentes. Os processos de certificação em curso, são o exemplo de uma atitude pró-ativa. Internamente estamos a evoluir. Agora na interação com outras instituições, começa a surgir problema. Aquilo que para mim é importante, para outra pode não ser. Se calhar eu tenho uma atitude pró-ativa e a outra instituição não tem. Mais uma vez isto faz sentido se for feito de uma forma global, de acordo com os interesses de cada organização. Todas as organizações que partilham dados devem participar ou iniciar um processo desta natureza. Tem que ser uma iniciativa conjunta, um compromisso conjunto, forçosamente. Internamente a sua implementação depende de decisões do topo das organizações.
P5.V1.1 – P4INEM#08	Sim, pode contribuir para sair da teoria.

	Como fez o sistema de saúde de Hong Kong. Eles têm neste momento integração completa dos dados clínicos, de todos dados dos doentes, e sempre que alguém, seja quem for acede nem que seja à morada ou ao número de telefone, a pessoa é notificada de alguma forma. Não chega apenas as pessoas darem autorização [consentimento]. É um primeiro passo obviamente, mas não chega. Porque a assimetria de informação que existe entre quem está a pedir autorização e quem está a dar autorização é de tal maneira grande, e o que as pessoas anteveem entre o ter a ganhar ou a perder, não se consegue avaliar, a única forma é dizer às pessoas " você está a dar autorização, mas sempre que alguém estiver a consultar a sua informação, você sabe". Sempre que os dados são fornecidos a uma terceira pessoa, o doente é informado. Em relação ao consentimento, aqui, às vezes é necessário inverter um bocadinho o mecanismo para ser eficiente - se eu estou à espera da pessoa me dar [o seu consentimento] posso parar um processo. Como a pessoa já autorizou e sabemos que aquilo é para atingir um fim que é bom para a pessoa, o processo não pode esperar pelo seu consentimento [...]. Podemos questionar se todas as pessoas têm acesso a mecanismos para autorizar o acesso ... é complexo. Resumindo este princípio da responsabilidade pode funcionar como um catalisador para estas matérias.
P5.V1.1 – P1HFF#01	Só faz sentido pensar em privacidade e segurança se eu tiver elementos ativos (informação, um computador, uma pessoa, um software). Ou seja, a importância de termos uma matriz de afetação de responsabilidades. E isto existe muito pouco. Mas é muito importante a sua definição. Dai que estou completamente de acordo com este princípio (o da responsabilização). Senão a desresponsabilização é total. Se eu tenho um responsável atribuído para a gestão de um sistema de gestão de bases de dados, eu tenho que assegurar que no ecossistema o seu responsável está preparado para preservar e proteger este bem/ativo. Agora se houver uma diretiva a sensibilizar para este princípio, este é interoperável entre organizações.
P5.V1.1 – P2HFF#02	Sim. Deveria ser desencadeado ao nível do ministério, deveria haver uma obrigação, uma portaria, uma recomendação para que em todas as instituições seja criado um gabinete que se preocupasse com este tipo de questões e que incluísse várias valências incluindo o gabinete jurídico, direções clinicas, responsáveis pelos sistemas de informação e responsáveis administrativos. Esta atitude por parte das organizações permitiria passar para fora uma mensagem de confiança. Isto só faz sentido se envolver todas as organizações. Promove mais a colaboração entre as instituições com base nas suas experiências.
P5.V1.1 – P2HFF#03	Eventualmente sim. Tem que vir de nível superior. Aquilo que tem acontecido, olhando para os últimos 15 anos, claramente os ganhos com aquilo que é levado à prática de uma forma transversal, mais rapidamente com ganhos em termos de escala, é aquilo que vem de cima para baixo. Pode ser um grupo que seja criado no seio da administração central que depois em colaboração com quem está no terreno possa aqui redigir um conjunto de normas que depois possam ser implementadas nos diferentes sistemas hospitalares. E também supostamente pondo em prática nos sistemas da tutela. Dizer que os hospitais têm que fazer isto e depois sou obrigado a usar um sistema que vem de cima e não tem nenhum desses desígnios, temos exemplos sito todos os dias. Passa de facto por evangelizar, nas reuniões a nível nacional, nas reuniões dos conselhos de administração a nível nacional. Este tema tem que ser colocado sempre de cima para baixo. Nunca um hospital se vai preocupar com isso e ativar o princípio da responsabilidade. Outro driver excelente da mudança são os contratos-programa - tem que existir algum tipo de indicador para medir a qualidade, a exigência, a maturidade, de forma a ser possível mensurar se um hospital está de facto a pôr em prática ou não as medidas ao nível da privacidade. É necessário dar alguma enfase à importância desta questão, antes de comessem a surgir casos de "polícia".
P5.V1.1 – P4HFF#05	Nós, internamente já não estamos na teoria. Monitorizamos já a nossa própria privacidade. Temos projetos comuns também no

	âmbito da privacidade, como a PDS, com um conjunto enorme de informações que saem do hospital diariamente, com vários processos, várias rotinas diárias que disponibiliza informação ao exterior, assumindo que a privacidade está assegurada. Nos dias de hoje a privacidade é uma questão tão técnica como de gestão. Ninguém melhor que o nível executivo para colocar o princípio da responsabilidade em prática. Mas compete à área técnica a sua execução e garantia do cumprimento deste princípio. O demonstrar para o exterior que existe por parte da organização uma responsabilidade em matéria de proteção de dados é sem dúvida uma função de gestão, uma orientação estratégica. Agora, a sua implementação depende de uma equipa multidisciplinar. Nos temos feito alguns progressos neste sentido nos últimos tempos. Temos uma comissão de informatização clinica, que avalia os projetos no âmbito da confidencialidade. Temos um processo de aprovações superiores para a informação que é disponibilizada ao exterior. Tem que haver competência nesta área também as tecnologias, nos sistemas da informação.
P5.V1.1 – P1SPMS#02	Segundo a nossa experiência, muitas das instituições só atuam por obrigação. Infelizmente algumas são aconselhadas a implementar determinadas políticas, mas alegam que não têm o tempo para o fazer, que têm outras prioridades. Acredito que havendo um despacho, uma regulamentação, que obrigue a essa implementação [do princípio da responsabilidade] pode ser o passo essencial para que se concretize. Deveria começar pelo topo das instituições, ser precedido por quem toma a decisão. Depois estamos da falar de sistemas de informação, os hospitais têm os seus sistemas de informação, e o seu representante poderia iniciar o processo a este nível, e depois escalando. Obviamente teria de ser criada a condição para passar essa informação até aos profissionais. Se o processo iniciar debaixo para cima, provavelmente o projeto nem sequer vai ser considerado, pois interessam outros indicadores mais prioritários. No caso da privacidade não existe um retorno efetivo. Uma diretiva nacional poderia iniciar este processo a nível nacional, tanto para o setor público como privado, que normalmente passa sempre ao lado. Poderíamos depois esbarrar com uma falta de preparação das organizações para estas questões. Na implementação de uma norma a nível nacional, algumas pessoas vão ter dificuldade em a compreender. Neste caso a informação tem que fluir até às unidades mais pequenas. Não seria uma má ideia faze-lo a nível nacional, mas teriam de trabalhar todos os intervenientes como as ARS: Seria necessário uma auditoria para perceber se está a ser implementado ou não, se existem dificuldades a implementar-se as medidas. Se for a nível local nós nunca vamos conseguir saber se foi implementado com sucesso. Alguém tem que fazer essa auditoria. Cada unidade pode implementar apenas as medidas que acha mais adequadas.
P5.V1.1 – P2SPMS#03	É difícil, mas pode ajudar. É um bom princípio. Não é fácil muitas vezes perceber quem é o responsável. Quem é o responsável pelos dados. Hoje em dia é algo que é muito claro. Apesar da SPMS ter um cariz muito operacional, é intenção nossa fomentar este principio. A nossa vontade é transpor a nossa política de segurança interna para uma política generalista do ministério que obrigue as entidades a terem alguns princípios. Definirem a sua própria política interna, e aqui o princípio da responsabilidade deveria ser replicado. Ainda assim existiriam enormes dificuldades operacionais para implementar esta intenção, mais questões organizacionais do que técnicas, de formação das próprias pessoas. É necessário que as pessoas percebem o âmbito e a pertinência das questões. Existe um desconhecimento completo sobre a legislação e sobre os processos. Nós fizemos um survey sobre segurança, e as pessoas desconhecem alquilo que é do mais elementar. Significa que há muito trabalho a desenvolver, até do ponto de vista formativo, dos responsáveis. As pessoas acham que podem fazer uma exploração e entrega de dados a terceiros, de ânimo leve. Normalizar estas situações

	pode significar que alguém está a querer "empatar" o sistema. Falta muita preparação nesta matéria. Os responsáveis deveriam ter mais conhecimento sobre dados e sobre como utilizar esses dados. PODE SER CULTURA DE PRIVACIDADE ! Apesar de muitas pessoas conhecerem a legislação, na prática às vezes as coisas não são suficientemente claras para aplicar a legislação. Muitas das vezes não é fácil de identificar o responsável, quanto mais aplicar legislação.
P5.V1.1 – P2SPMS#04	Entendo o conceito e acho que este princípio poderia ter um efeito prático positivo. Olhar para aquilo que é a legislação, perceber que implicação prática tem, e começar a implementar algumas medidas, pode ser um 1º passo importante.
P5.V1.1 – P4SPMS#05	Antes da lei de proteção de dados, as entidades já eram responsáveis pela proteção de dados. E porquê? Este princípio não tem que ser ativado, ele já lá está. Se é exercido ou não, ou se é transformado num componente relevante para o negócio, é diferente. Antes da lei de proteção de dados, já havia dados, digitais e em papel. Porque já era importante para as pessoas nas organizações, preocuparem-se com esses dados, no acesso e na segurança destes dados, porque ainda que não infringissem num litígio, num comportamento ilegal, infringiriam eventualmente, os seus profissionais ou outros, em risco organizacional. Já nessa altura, saber-se na praça pública informação clínica sobre um determinado indivíduo, era mau do ponto de vista da reputação da instituição, que tem que salvaguardar a saúde do individuo. Ora a saúde do individuo, até certo ponto, inclui a sua privacidade. Um individuo em que a sua privacidade seja comprometida, fica "doente" na sua esfera social. Portanto como entidade de saúde, muito antes da lei de proteção dos dados, sempre houve a preocupação de cuidar dos dados. Ou seja não é necessário ativar o princípio. Ele já lá está. Agora o que é que ele significa na prática? O que fazem as pessoas quando entram no local de trabalho pela primeira vez? Têm cursos de formação? São sensibilizadas para esta questão? Quando há um problema, este é discutido até à dimensão de alteração de comportamento e processos? Tudo depende da vontade dos atuais gestores das unidades. Não depende nada da lei ou da CNAPD. Só depende da boa prática de gestão. Já hoje é melhor para uma entidade gerir bem os dados, do que gerir mal.
P5.V1.1 – P1HES#01	O processo clinico eletrónico, onde temos as informações mais sensíveis em termos de proteção de dados, tanto a aplicação que utilizamos, assim como a base de dados são acedidos através de autenticação segura, em que tudo que é apagado, alterado e consultado fica tudo registado. Em termos de regras de segurança e da forma como o sistema está desenhado, tinha a ideia que nós teríamos garantido a segurança da informação clinica. Contudo, quem é que consegue garantir que um determinado médico, não imprime e leva a informação que pretender para fora do hospital. Como é que eu garanto sito? São situações que têm a ver com o dever de cada profissional, com o sigilo. As pessoas sabem que não podem imprimir e levar um processo clinico. Mesmo quando o tentam fazer, o sistema apresenta uma mensagem a informar que de acordo com as regras de segurança da instituição não deveriam imprimir um relatório clinico. É um alerta e pode não ser suficiente. Estamos a falar de medidas para garantir que a informação é utilizada de forma segura e por quem a deve utilizar. Nós já trabalhamos um pouco no sentido do princípio da responsabilidade, até porque já temos vários exemplos de coisas que nós já fazemos para tentar garantir este princípio de alguma forma. Poderíamos fazer sim, nós e toda a gente, mais ações de sensibilização. A dinamização de um programa desta natureza depende para quem é dirigido. Se for para falar com médicos deve ser dirigido por um médico. As pessoas ouvem melhor os seus pares, do que se um responsável pela informática lhes disser quais as políticas a implementar, e a forma de as implementar. A informação é sempre melhor recebida quando vem dos seus pares. Temos que

	encontrar dentro de cada grupo profissional a pessoas com mais apetência para este tipo e coisas. Também acho que nestas questões a gestão de topo tem que estar sempre envolvida. Veja o exemplo da implementação do ALERT no HES. Estava condenado ao fracasso e toda a gente dizia que era impossível a sua implementação. Os médicos não queriam passar da segurança dos registos em papel, em que o papel com facilidade se rasga, para um processo clinico eletrónico onde uma vez registada a informação não pode ser eliminada com facilidade. Neste caso a gestão de topo envolveu-se como nunca, foi para o terreno e falou com todas as pessoas, e ao mesmo tempo encontrou *players* dentro de cada um dos grupos profissionais, formando um grupo de trabalho que depois falava com os seus pares. E o processo funcionou bastante bem. Em qualquer um destes temas, a segurança, a privacidade, a política de responsabilidade, faz todos o sentido iniciar na gestão de topo, não tenho nenhuma dúvida sobre isto, mas depois encontrar os *players* certos dentro de cada grupo profissional que transmitam aos seus pares qual é que é caminho, e as mais-valias daquele caminho.
P5.V1.1 – P2HES#02	Faz todo o sentido e é importante este princípio. Acho que as pessoas estão pouco sensibilizadas para o nível da proteção de dados. Não se preocupam muito quem tem acesso aos dados e sobre que condições. Não deveria ser assim, as pessoas têm que ter responsabilidade a este nível. Esta questão da privacidade dos dados funciona muito à antiga – surgiu um problema e depois vamos ver o que podemos fazer. Existe muita falta de conhecimento, até da própria legislação de proteção de dados. Um programa de responsabilidade desta natureza, que contemplasse um conjunto de medidas obrigatórias, medidas gerais que permitisse às pessoas perceber aquilo que é a proteção de dados e a importância da sua privacidade, teria que vir do topo da instituição, do nível da administração, em colaboração com os responsáveis pelos sistemas de informação, gabinete jurídico, e outros responsáveis. Poderiam disponibilizar esta informação na Intranet, ou através da realização de um *workshop*. As pessoas poderiam vir a ter mais cuidado depois de informadas.
P5.V1.1 – P2HES#03	Este é um princípio que deveria já estar ativado. Seria um caminho para por em prática as questões da proteção e dados. Assim quando chegar a legislação já tínhamos algum conhecimento que nos permite adaptar com mais facilidade. Acho que tudo que seja sobre proteção de dados e segurança é sempre pouco.
P5.V1.1 – P4HES#06	Poderá haver um alinhamento dos grandes princípios de privacidade entre instituições. Um compromisso entre instituições a nível nacional para com a proteção e dados. Mas, mais uma vez, não vale a pena falarmos de compromisso se os instrumentos não estiverem disponíveis e configurados. É só uma questão de configurar os instrumentos. Nós estamos muito longe de ter esse problema [da fuga de informação]. Este problema só faz sentido se tivermos instrumentos que nos deem garantias. Se tivermos estes instrumentos, a seguir vamos saber se nos detalhes nós conseguimos melhorar alguma coisa. Mas os instrumentos que nós temos não nos garantem qualidades mínimas. Deveria haver grandes diretrizes ao nível da proteção de dados uma vez que as aplicações atuais não garantem a segurança da informação. Não compete às instituições criar barreiras às medidas legislativas. E as aplicações atuais, onde se inclui a PDS, foram criadas como medidas legislativas. O meu problema atualmente não é a utilização secundária dos dados (usar os dados através de um estudo de investigação cientifica), ou outra situação. O meu problema é que quem quiser usar os dados, usa-os, sem autorização de ninguém. É neste domínio que deveríamos atuar, estar precavidos. A nível local não podemos fazer nada, só se formos contra a legislação. O ministério da saúde implementou uma coisa que se chama PDS. A PDS não tem garantias de privacidade. O que é que eu posso fazer? É legislação. Vou dizer ao ministério que não

	faço o que diz a legislação? Se o ministro da saúde for algum dia a um hospital público, eu no dia seguinte consulto toda a informação sobre ele. Se eu tiver o seu nome, consigo no sistema saber tudo sobre si. Esta situação é preocupante, dramática, não deveria ser permitido. Há aqui dois princípios: o princípio de que a informação deve estar disponível, porque ela pode ser útil para tratar um doente, e há o princípio da proteção dos dados. Cada um tem direito a que os seus dados estejam protegidos. O conflito destes dois princípios existe. E deve haver uma atitude de responsabilidade ao criarem mecanismos. O que foi feito foi um mecanismo (a PDS) que respeita o princípio de acesso aos dados, e ignora o princípio da confidencialidade. Eu não concordo com isto. Mas não me compete outra coisa senão implementá-la.

P5.V2.1

P5.V2.1 – P2ULSNA#02	Temos vindo a falar da necessidade imperiosa do dicionário de privacidade. (interrupção) Antes de existir algo do ponto de vista técnico têm que existir em papel um conjunto de regras, definidas com base na legislação portuguesa, analisando o que é possível e exequível dentro deste tipo de instituição realizar. Uma equipa pode depois ser criada para analisar e avaliar os diferentes processos, ou processos escolhidos aleatoriamente.
P5.V2.1 – P2ULSNA#03	Com a segurança é possível testar a sua conformidade. Na privacidade dos dados esta também pode ser testada, simulando situações.
P5.V2.1 – P4ULSNA#06	É possível, e desejável, fazer esta análise contínua de conformidade. Não deve haver receio no escrutínio das tarefas ou situações, uma vez que esta análise pode ser uma melhoria para a organização, salvaguardando outros eventos que eventualmente possam questionar a proteção.
P5.V2.1 – P2USF#02	Faz todo o sentido que a análise de conformidade seja contínua. É importante perceber se as nossas ferramentas, processos estão de acordo com a legislação.
P5.V2.1 – P4USF#05	Sim. Fazer auditorias é importante. Saber se está a ser cumprido certas medidas. Hoje em dia funcionamos muito com auditorias, tanto internas como externas.
P5.V2.1 – P2INEM#03	Eu costumo dizer que não basta implementar um qualquer sistema e deixa-lo a correr. Há que ir verificando se ele está a cumprir e está a fazer o que é esperado fazer. Sim, a análise de conformidade regular também deveria ser uma prática comum para a proteção de dados, verificar se está de acordo com a legislação, regulamentos ao nível interno. Desvios vão acontecer sempre, ou são passíveis de acontecer, dai a necessidade de uma verificação regular.
P5.V2.1 – P2INEM#04	Uma análise de conformidade à proteção de dados seria útil. Permite-mos averiguar se a proteção de dados está de acordo com as exigências existentes. É necessário mais monotorização. No fundo as soluções são implementadas e depois não são monitorizadas com a atenção devida. Não se faz habitualmente, só se faz mesmo por necessidade. Fazemos de uma forma mais apertada uma monitorização no início dos projetos, mas depois acabamos sequer por ter disponibilidade para continuar. É uma grande dificuldade. Ainda por

	cima os recursos humanos são limitados e temos que abarcar assuntos diversos.
P5.V2.1 – P2INEM#09	Sim a análise regular da conformidade da utilização de dados seria uma ferramenta fundamental. Em relação a alguns sistemas fazemos regularmente alguns testes de análise das boas práticas de utilização. Permite analisar se estamos a cumprir com todas as boas práticas, ou não. Corrigimos o que está mal. Dentro do domínio dos dados deveria ser igual. Não deveríamos ficar limitados a infraestruturas, equipamentos. Em termos de dados esta análise é mais exigente.
P5.V2.1 – P2INEM#10	Sim esta ferramenta faz todo o sentido - a análise da conformidade. Faz sentido regularmente fazer uma análise de conformidade das políticas de privacidade. Só assim é que posso garantir a eficácia das medidas. Eu só consigo garantir a eficácia se reavaliar regularmente.
P5.V2.1 – P4INEM#08	O primeiro passo para eu ter segurança é conhecer quem consultou os meus dados – porque é que um determinado médico, de um determinado hospital está a ver o meu caso? Obriga a que os sistemas de informação garantam a rastreabilidade dos dados pessoais, em diferentes níveis. A análise da conformidade também se deveria adaptar ao nível da proteção de dados. Temos que ter em atenção que quando intervimos numa análise desta natureza podemos ter duas perspetivas: uma perspetiva de fiscalização ou uma perspetiva de auditoria, que tem o objetivo de melhoria continua. Obviamente num plano a implementar tem que haver uma grande preocupação em sensibilizar as pessoas para esta área, tem que haver uma grande preocupação em utilizar ferramentas que permitam o diagnóstico e a rápida resolução das questões diárias, e depois passar para o nível de exigência ao nível do certificado de confiança.
P5.V2.1 – P2HFF#02	Na segurança é um ciclo de evolução que é positivo. Em relação à proteção de dados, é viável, deveria existir também uma matriz de análise. Neste momento não temos nenhuma matriz/framework objetiva para este tipo de análise. O que causa muita dificuldade é o facto de a pessoa não saber para onde deve caminhar. O conhecimento de todos os processos de recolha e tratamento de dados é uma boa base de atuação. Juntando aquilo que é legislação estamos em condições de perceber se estamos ou não de acordo com a legislação de proteção de dados. Esta análise regular da conformidade da proteção de dados depende de um guião, de um padrão, tal como já se faz para a segurança.
P5.V2.1 – P2HFF#03	Aquilo que é prática dominante na segurança de análise de conformidade. Tem de se movimentar para os dados. Estamos a desenvolver um processo de acreditação, que vai decorrer aos diferentes níveis dos processos. Mas este tópico é um tópico ainda muito limitado. Ou seja, ainda tem a maturidade, nem se exige neste processo de acreditação a questão da privacidade dos dados.
P5.V2.1 – P4HFF#05	Para a área de proteção, privacidade dos dados deveria haver à semelhança da segurança, uma análise de conformidade continua. No âmbito restrito de uma organização a monitorização da utilização de dados deve ser continua, assim como a implementação de medidas para termos essa garantia.
P5.V2.1 – P2SPMS#03	A análise de conformidade deveria ser uma ferramenta também aplicável à privacidade dos dados. Só com auditoria se consegue verificar se se cumpre. Em termos de auditoria de conformidade aquilo que se audita são as regras existentes. Daí que seja passível de implementar uma análise de conformidade em relação à segurança dos dados. Em relação à privacidade dos mesmos penso ser mais complicado uma análise de conformidade.
P5.V2.1 – P2SPMS#04	Auditar-se regularmente aquilo que é a utilização dos dados, à semelhança da segurança seria vantajoso. Não temos ainda

	ferramentas para isso. Ferramentas para perceber se estamos a fazer um bom trabalho, em matéria de proteção e privacidade dos dados. Se percebermos quais são os riscos em termos de informação, podemos depois verificar regularmente se estamos a conseguir eliminar o risco. Neste momento já estamos com várias iniciativas de auditoria relacionadas com a qualidade dos dados. O próximo passo vai ser sem dúvida a parte da proteção destes dados.
P5.V2.1 – P4SPMS#05	Em primeiro devem ter uma análise de segurança. Muitas instituições [na área da saúde] ainda não têm esta prática. É facílimo chegar a um computador qualquer sem uma login a um hospital qualquer, vestido com uma bata qualquer! Se não se identifica à entrada num edifício, se as pessoas são ou não trabalhadoras deste edifício, então começam aqui os problemas de segurança.
P5.V2.1 – P2HES#02	A análise de conformidade como ferramenta deveria também estar a ser aplicada à proteção de dados. Vai de acordo com o que já disse anteriormente. A aplicação das normas ISO27001 por exemplo, que fala especificamente com a componente de conformidade da segurança. A aplicação desta norma à gestão da informação não é fácil. A definição das medidas de proteção dos dados não é fácil. A análise de conformidade acaba por ser uma auditoria. Auditoria de analisar e corrigir os problemas identificados.
P5.V2.1 – P2HES#03	A maior preocupação que deveríamos ter em relação aos dados é a sua encriptação total. Devíamos estar a adaptar esta análise de conformidade também aos dados. Verificar se os dados estão a ser utilizados de uma forma correta, se não existem erros na informação, se estes não foram adulterados. São necessárias ações preventivas.
P5.V2.1 – P4HES#06	Tal como olhamos para a criticidade dos sistemas informáticos deveríamos olhar também para a criticidade dos dados. Num suporte em papel, após a consulta, isto vai para o arquivo e ninguém o pode consultar. Só o podem consultar quando vier a outra consulta. Se outro médico quiser aceder a este processo tem que pedir autorização. Tem que demonstrar que tem uma razão legítima para aceder à informação em papel. Neste momento em suporte informático, eu faço um registo e no segundo seguinte qualquer pessoa do país pode aceder ao registo. Isto não faz sentido, porque se nós temos um processo aberto e toda a gente consulta a informação, no momento em que quer, para que é que nos vamos preocupar com o acesso aos dados para estudos clínicos? Está tudo aberto. Devemos olhar para os sistemas com um acesso de uma forma controlada e não de uma forma totalmente aberta, caso contrário entramos num caos. Mas a legislação fez o contrário. Obrigou-nos a usar uma plataforma e a darmos acesso aos nossos dados. Temos sido bastante críticos em relação a todo este processo. Estarmos a falar de confidencialidade no mesmo momento em que temos a PDS, é o mesmo que estarmos a falar de como vamos "*controlar o furto num país onde é obrigatório toda a gente ter as portas abertas*". Quando não se pode impedir ninguém de entrar não podemos estar preocupados com a confidencialidade. É evidente que se a PDS garantisse os principais mecanismos de proteção aumentava a confiança das organizações nos seus serviços. Eu não consigo, é entender como se desenvolve a PDS sem que a confidencialidade dos dados não esteja garantida. Mesmo que a PDS monitorize a utilização dos dados, eu posso sempre ler os dados utilizando um *login* de um outro utilizador qualquer. Se pretender agir com má-fé não vou usar o meu *login*. Andamos anos para garantir a confidencialidade, arquivos onde ninguém entra fisicamente sem autorização, processos clínicos utilizados por profissionais ao abrigo do sigilo profissional. Só aquelas pessoas podem utilizar os processos em papel.

P5.V2.2

P5.V2.2 – P2ULSNA#02	É necessário definir a realizada. Apesar da importância da privacidade, não fazemos nada para a defender e neste tipo de instituições, nós gostamos muito das questões da privacidade, mas a nível nacional não existem sistemas implementados para defender os dados dos nossos utentes. Tal como na segurança a criticidade é importante. É importante sempre que possível anonimizar o utente, protegendo assim o que está por detrás desse utente.
P5.V2.2 – P2ULSNA#03	Através de uma análise periódica sobre transferências, sobre tudo aquilo que é feito de dentro para fora.
P5.V2.2 – P2USF#02	A qualidade dos dados é determinante. Dados mais sensíveis obrigam a uma maior preocupação. O volume de dados tratados, não considero importante. Importante sim é se os dados são ou não críticos. Se conhecermos bem o cenário de utilização, o risco associado, poderemos prepararmo-nos melhor.
P5.V2.2 – P2INEM#03	A sensibilidade dos dados vai definir a prioridade. Se temos dados muito sensíveis em que tem que haver a garantia que não saem daquele circuito, então tem que se ter uma verificação nitidamente mais apertada que para os dados, que não sendo tão sensíveis, não são críticos se algo acontecer.
P5.V2.2 – P2INEM#04	Poderá ser a sensibilidade e exposição dos dados, a forma como poderão estar a ser utilizados. A sua maior ou menor confidencialidade obrigam a que se faça um controlo, assim como a sua maior ou menor exposição.
P5.V2.2 – P2INEM#09	O conhecimento do ciclo de vida dos dados é importante. O facto de a sensibilidade dos dados ser mais crítica [não é o caso dom INEM], como dados clínicos de hospitais, vai determinar o que é prioritário que termos de auditorias. Isto implica que haja pessoal que tenha formação específica nesta matéria, o que não acontece. No nosso caso onde temos vindo a perder pessoas, e para fazer mais do que a gestão corrente, é necessário técnicos. Limitamos a assegurar o que temos.
P5.V2.2 – P2INEM#10	Sei que nós lidamos diariamente com imensa informação de cariz pessoal. Trabalhamos diariamente com muitas pessoas. Onde temos informação pessoal, sensível, garantidamente tem que ser dada mais atenção. Informação mais de transacções, de gestão, não será necessário a mesma periodicidade. Quando um processo é mais crítico, quando uma ferramenta é mais crítica é necessário uma maior atenção. Normalmente, a noção que eu tenho, é que em relação aos dados isto não é feito. Não é analisada a utilização dos dados. Nós não olhamos para os dados com a atenção que eles merecem.
P5.V2.2 – P2HFF#02	Tem a ver com a maturidade da instituição. Existem áreas onde os dados são mais sensíveis, o que implica que mais regularmente se faça esta análise de conformidade. Ou seja depende muito do tipo de dados. Há aqueles dados que são objetivos. A facilidade de acesso aos dados também é importante. Por exemplo analisar diários clínicos já é muito mais difícil. A privacidade destes dados tem que ser maior. Com uma análise de risco, como já falamos, haveria um maior conhecimento sobre o risco de cada situação de utilização de dados e se houver uma área onde existe por exemplo uma maior intensidade de utilização de dados deve-se incidir com mais medidas.
P5.V2.2 – P2HFF#03	Se eu tenho um sistema que é critico, um depósito de dados que é critico, periodicamente vou verificar se as medidas estabelecidas de segurança estão ou não estão a ser cumpridas. Em relação aos dados se eu optar por uma política de análise de conformidade continua, e face à maturidade em que nós estamos, garantidamente a sensibilidade dos dados. Áreas críticas em

	relação à informação. Toda a informação que tiver impacto, sendo que a informação é poderosa em termos económicos, que tem relação com seguradoras, com questões legais, tem que garantir que essa informação está mais protegida. Agora no caso de um hospital tudo que é informação clinica, pura e dura, é crítica. Assim como toda a informação relacionada com processamento de vencimentos, onde é suposto não ser vista por qualquer um. Realmente há aqui algum rigor e algum sigilo, mas é diferente da informação clinica. Existe uma relação direta com a análise de risco. Este é um novo paradigma. O aceso à informação de qualquer local. E o acesso a grandes volumes de informação. Dantes, em suporte papel, isto era impossível de concretizar. À medida que o repositório surge, vai tendo mais valor, estas questões começam a colocar-se. Exige-se uma maior transparência em relação a estas questões.
P5.V2.2 – P2SPMS#03	Depende da dimensão do que estivermos a falar e do seu impacto. Depende muito do sistema em si, do tipo de dados que estamos a utilizar, da sua criticidade. Tem muito a ver com a análise do risco, é determinante. Depende muito daquilo que é o impacto do que é uma falha de privacidade sobre aquela informação. Teria que ser como no setor financeiro, com uma preocupação, uma maior proteção e uma maior monitorização da utilização dos dados.
P5.V2.2 – P2SPMS#04	Onde existir informação mais critica, concordo que se devesse investir mais neste tipo de auditoria. Informação do domínio administrativo não é tão perigosa como informação do domínio clinico, em termos de privacidade. Onde tivermos dados mais sensíveis deveria haver uma maior proteção. Cenários de partilha de dados também deveriam ser auditados com mais frequência.
P5.V2.2 – P2HES#02	Há um conjunto de critérios a considerar. Onde houver informação mais sensível, provavelmente tem que se analisar mais vezes a sua conformidade.
P5.V2.2 – P2HES#03	Com informação mais critica, nomeadamente análises clinicas, deve ser analisada a sua conformidade com mais regularidade. É sempre importante fazer a monitorização e procurar avaliar dos riscos, e tentar perceber o que é que pode falhar. O problema aqui é mesmo o tempo necessário para realizar esta tarefa.

P5.V2.3

P5.V2.3 – P2ULSNA#02	Claro. Pode permitir traçar mapas de tendência de acesso, determinadas utilizações específicas que não pensávamos existir. Este tipo de avaliação permitiria conhecer claramente que tipo de procura de informação ou dados é suspeita, e nós não temos ferramentas em prática com este objetivo. A identificação de padrões seria importante, com base na identificação dos utilizadores, perceber com base numa linguagem de análise, que dados devem ser monitorizados. O tornar publica desta informação, cria do outro lado uma maior confiança no sistema de informação.
P5.V2.3 – P2ULSNA#03	Eu acho que sim. Contudo esta publicação depende da necessidade de ter a certeza que temos assegurado estes procedimentos de conformidade. A certificação surge neste caminho. Uma mais-valia para a própria instituição, porque havendo resultados positivos, seriam benéficos para a instituição.
P5.V2.3 – P2USF#02	Sim sem dúvida, faz todo o sentido. Concordo com a publicação destes resultados.

	Diga-mos que “alertar”, seja a publicação boa ou má. Permite comunicar o que temos e onde não cumprimos. E se não cumprimos vamos ter que mudar. Acho que todas as organizações deveriam fazer isto, e definir objetivos neste domínio. Ser responsáveis em reconhecer que não estamos a cumprir aqui e aqui, mas vamos fazer os possíveis por cumprir. Alem de aumentar a confiança entre as organizações, se estes dados são publicados não apenas internamente através das intranets, e são publicados no exterior, aumenta a confiança para os utentes, para o próprio cidadão.
P5.V2.3 – P2INEM#03	Poderá ser vantajoso, à semelhança da segurança. Pode trazer mais descanso e garantias às pessoas ao fornecerem um conjunto de informação.
P5.V2.3 – P2INEM#04	Era positivo, mas apenas numa perspetiva de deixar as pessoas mais tranquilas em relação à forma como aquela organização trata os dados. Entre as organizações poderia criar pontos de confiança, alias uma das coisas muito sensível entre as organizações é precisamente a desconfiança em relação à segurança, o que leva a muita relutância a se fazer intercâmbio de informação, mais da parte dos médicos, que se procuram defender em relação à exposição de determinada informação. No nosso caso, desde alguns anos que tentamos trocar informação, nomeadamente com os hospitais, e não conseguimos. Sentimos de facto uma grande indisponibilidade, não propriamente da organização hospitalar, mas sim das pessoas que lá trabalham […].
P5.V2.3 – P2INEM#09	Da mesma forma em que a certificação numa norma ISO dá confiança, da mesma forma a publicação desta análise poderia promover o mesmo. Se esta constituir uma boa prática deve ser publicada. Caso contrário deverá ser utilizada esta informação para corrigir os problemas identificados. Neste período não é aconselhado a publicação destes resultados. Dentro da área da saúde, parece-me a mim que, se esta análise for feita, é de todo vantajoso haver esta publicação, promoção dos bons resultados, após a correção daquilo que não estiver bem. Antes não. À semelhança do que já se faz com os testes de robustez para as infraestruturas, deveria pensar-se em algo semelhante para os dados, para a sua proteção.
P5.V2.3 – P2INEM#10	Esta questão é sempre um “pau de dois bicos”. Eu sou daquelas pessoas que acha que estas questões devem ser sempre públicas. Não faz sentido esconder as coisas. Agora quando não se cumpre, quando as coisas não correm bem é necessário assegurar que estamos mesmo a resolver. É importante que as pessoas saibam que em que instituições estamos a ser eficazes, e em que instituições se está a trabalhar no sentido de serem eficazes nesta matéria. Esta publicação pode ter um efeito positivo para a organização, faz todo o sentido.
P5.V2.3 – P2HFF#02	Tem que haver transparência. Se não houver transparência do que é que nos serve a privacidade? A publicação destes resultados aumenta a confiança que as pessoas podem dar a essa organização.
P5.V2.3 – P2HFF#03	Sim, demonstrar que estamos de acordo com um conjunto de requisitos. Num processo de qualidade, ou em processos de cumprimentos de indicadores, demonstrar o que fizemos é importante. Por exemplo num processo de melhoria de qualidade da informação é importante mostrar aos clínicos os registos clínicos da sua responsabilidade. E neste processo detetamos vários problemas. Erros na informação. Profissionais atribuídos ao serviço errado. Começa-se agora a detetar problemas na qualidade da informação, fruto da transparência. A transparência é essencial à confiança na organização, e para que os próprios profissionais façam a sua própria auto validação da qualidade da informação.
P5.V2.3 – P2SPMS#03	Sinceramente é uma pergunta que eu não sei. Diria que por vezes pode não ser benéfica, porque pode criar algum alarmismo em

	quem desconhece o processo. Porque dizer que não está em conformidade numa área de privacidade é complicado. Até para a opinião pública em geral conseguir perceber exatamente o que é aquela não conformidade e o que ela pode representar e qual é a probabilidade de ela acontecer. Os americanos publicam as falhas de segurança e as pessoas devem ter processos de notificação. No caso de existir conformidade em relação a todos os requisitos externos, aqui a sua publicação poderia transmitir alguma confiança aos utilizadores externos, aos utentes do SNS. No caso da não conformidade poderia causar uma desconfiança. Teria as suas vantagens e certamente as suas desvantagens. Não seria contudo por este facto que os utentes deixariam de se inscrever para uma cirurgia. Há valores mais altos que se levantam.
P5.V2.3 – P2SPMS#04	Acho importante a publicação deste tipo de análises e resultados em relação à proteção de dados. As pessoas poderiam desta forma ficar mais conscientes deste problema. As pessoas hoje em dia nem se apercebem das consequências.
P5.V2.3 – P2HES#02	Eu acho que a publicação destes resultados deve acontecer e deve ser vista num sentido pedagógico. No sentido de corrigir algumas falhas que possam existir ao nível daquela segurança. Com a publicação dos resultados as pessoas podem ficar consciencializadas com o problema. Demonstrar que o que foi feito até aqui, não foi feito da melhor forma, e que se aplicarmos novas medidas iremos melhorar. Devíamos estar a caminhar para "selos de garantia" ao nível da proteção e dados, e aí de certeza que as instituições iam promover estes selos de garantia.
P5.V2.3 – P2HES#03	É importante a publicação destes resultados. Contudo, depende para onde se publica. Não sei se o termo correto será publicar, e não informar. Informar as instituições intervenientes sobre os pontos de falha, que desencadeiem uma ação. Estando tudo bem desencadeia uma confiança em quem nos entrega os dados. Neste caso tem que se informar sem muitos aspetos técnicos. Deveria ser um requisito, as instituições provarem que cumprem com a legislação em relação à proteção de dados e à segurança. A certificação é um caminho. […] Não é necessário contudo uma exposição demasiada desta informação.

P5.V3.1

P5.V3.1 – P2ULSNA#02	A nossa experiência enquanto técnico de informática em sistemas deste tipo é praticamente nula. A partilha de informação que existe vem do ministério da educação e acabamos por não estar cientes do que é partilhado, do que é divulgado. Assumimos que as coisas estão a ser feitas da melhor forma, mas é verdade deveriam existir regras.
P5.V3.1 – P2ULSNA#03	Acima de tudo devem registar quem fez o quê. É importantíssimo o registo tanto para o bem como para o mal. Havendo problemas consegue perceber-se quem fez, o que é que aconteceu. No nosso caso não existe uma observação periódica destes dados a nível local. Para o contexto de colaboração este tratamento obrigatoriamente tem que ser mais exaustivo. Existe uma grande falha neste domínio.
P5.V3.1 – P2USF#02	As organizações hoje em dia têm orçamentos muito limitados para o IT. Uma solução desta natureza seria dispendiosa. Seria

	desejável uma maior interoperabilidade entre os sistemas de *account* das várias organizações. Apesar de ser pertinente que os sistemas registem detalhadamente quais os dados que um utilizador acedeu e alterou temos que ter confiança no utilizador. No domínio da saúde, já se consegue perceber quem acedeu e de onde acedeu aos dados. Em termos de privacidade é o início para se perceber que temos à disposição neste momento ferramentas que nos permitem pelo menos controlar o acesso às nossas aplicações, e se houver um problema nós conseguimos responder: nesse local, na hora tal, foi efetuada determinada tarefa. A base de dados na saúde (SINUS) é a espinha dorsal para vários sistemas e aplicações, e isto por si só obriga a uma atenção maior e a um rigor ao nível da segurança. Existem normas que têm que ser cumpridas. Temos que conseguir saber quem está a aceder aos dados, e isto é triado todos os dias.
P5.V3.1 – P2INEM#03	Estes sistemas são importantes para o contexto de partilha de dados. Só pelo facto de poder facilitar a partilha de dados, ao produzirem prova da utilização de dados, já são importantes. Se queremos ter partilha de dados, estes sistemas têm que funcionar integrados. Eu consigo controlar os meus dados, mas fico preocupado quando os meus dados transitam para outros sistema, que eu não sei como vão ser tratados lá, e isto é um deito da organização, saber como estão a ser tratados os dados. Se eu tenho requisitos de confidencialidade eu tenho que ter garantias que as outras organizações têm os mesmos padrões.
P5.V3.1 – P2INEM#04	Em determinado tipo de utilizações é um pouco isso que nós já fazemos, não só para acautelar os dados, como também para percebermos se a utilização que estão a fazer dos sistemas é a correta ou não, e também para percebermos que quando há um erro, exatamente onde é que ele está a ser gerado. Mas isto não cobre todas as necessidades. Com os dados a fluir cada vez mais entre sistemas, estes sistemas [*accountability*] têm que se adaptar. Eu perco o controlo sobre os dados. Idealmente estes sistemas [*accountability*] têm que começar a integrar-se uns com os outros, a partilhar informação, de modo a eu poder saber para os dados que saíram do meu sistema o que é que estão a fazer com eles. Por exemplo, no domínio da PDS, pediram-me que disponibiliza-se um web-service para um conjunto de dados. Eu não sei como é que estes dados estão a ser utilizados.
P5.V3.1 – P2INEM#10	Idealmente, os sistemas [de *accountability*] devem ser capazes de dialogar entre si. Na realidade em termos tecnológicos não me parece que seja fácil implementar uma coisa destas [o dialogo entre sistemas]. No mínimo estes sistemas devem ser capazes de controlar localmente os seus sistemas. O ideal é serem capazes de dialogar entre si. A partir do momento em que os dados passam para outro sistema, eu perco o "rasto" a estes dados. Tem que haver uma integração futura destes sistemas. Seria solução ideal.
P5.V3.1 – P2HFF#02	O registo de todas as tarefas realizadas localmente ou remotamente são uma garantia de que os dados estão a ser utilizados de forma correta. Os sistemas de account deveriam ser os responsáveis por este tipo de tarefa. Ao não existir legislação a obrigar a este nível de registo, este não é feito. Agora é importante perceber de forma granular o que se passou com a utilização dos dados. O problema aqui tem a ver com a tecnologia. Nós ainda temos alguns sistemas *legacy* em que não é possível ter isto. Implicaria um investimento tremendo. Quando passamos dados para um outro sistema, perdemos o rasto a esses dados. Quando falamos em identidade digital, deveria ser possível que todos os dados fossem assinados com um certificado digital. Seria uma ferramenta de privacidade fantástica. Nada me impede de que eu vá a uma base de dados e "adultere" um dado sem haver registo. Internamente já estamos no domínio dos sistemas de informação, a avaliar a qualidade dos dados que estão a ser registados. E esta avaliação da qualidade dos dados

	registados vai nos ajudar também muito em relação à privacidade. É necessário que estes sistemas evoluam do controlo dos utilizadores e dos serviços para os dados. A malha de colaboração depende de mecanismos que obriguem a tecnologia a colaborar.
P5.V3.1 – P2HFF#03	Eles são muito a prova de evidência quanto à utilização dos serviços. Consigo já chegar aos dados, no que toca a prova de evidência, provar que um utilizador alterou e utilizou estes dados. É o único instrumento que nós temos se houver algum problema de segurança. Ou seja, num caso de furto de informação conseguimos saber quem e quando realizou o furto. Mas primeiro temos que saber que fomos "assaltados". Muitas vezes funciona assim, havendo dúvidas vamos escrutinar. Não temos ainda mecanismos de previdência, de garantir que aquilo não é possível fazer. É difícil estes sistemas adaptarem-se aquilo que é cada vez mais a interoperabilidade entre organizações. O desafio é gigantesco. Porque nós não damos qualidade à informação, não atribuímos uma característica à informação, para a poder depois classificar e adequar. Simplesmente, nós enviamos a informação. E depois quando a informação vai para outro repositório, é o outro sistema que exerce o controlo, e que é diferente do meu. Isso é a realidade. Tem que haver uma interoperabilidade técnica a nível destes sistemas.
P5.V3.1 – P2SPMS#03	A sua evolução deve contemplar pelo menos a informação sobre quem acede aos dados, quem os altera, quem os cria. Na maior parte dos sistemas não existe este conceito. Quando os dados passam para um outro sistema externo, deve ser evocado em que contextos estão a ser passados. Deveria existir em termos de histórico. Deveria ser sempre possível rastrear os dados, mesmo para lá do nosso sistema. Pelo menos o contexto em que eles passaram para o outro sistema. Pela minha experiência o *accountability* é quase sempre realizado de uma forma isolada, com cada aplicação a fazer o seu registo. Este registo deveria ser centralizado uma vez que é um serviço essencial. Disponibilizar esta informação ao utente era relevante. Ficaria a saber quem acedeu à sua informação. No caso da PDS é possível saber quem acedeu à informação. Se todos os sistemas tivessem este tipo de abordagem seria fundamental. A partir daí eu sou dona da minha informação e sei quem é que está a aceder. O *account* de sistema, em que é registado a entrada e saída de um utilizador é nitidamente insuficiente. Tem que se ir mais longe em que é necessário registar quem acedeu à minha informação e em que contexto. É necessário perceber qual é fluxo de negócio dos dados. É no fundo um registo baseado nos dados e não apenas nos utilizadores. Ainda não temos isto.
P5.V3.1 – P2SPMS#04	O básico é que estes sistemas registem a entrada e saída do profissional, e depois todas as tarefas que realizou têm de ficar registadas. Agora esta informação com o tempo começa a pesar no sistema, sendo que temos que ter sistemas de reporting. Isto pressupõe um maior foco nos dados. Quando falamos de informação de passa de uma base de dados de um sistema para outra base de dados de um outro sistema, perco o rastro aos dados. Não sabemos o que é feito com os dados do outro lado. No fundo a PDS já começa a rastrear a utilização dos dados a nível nacional, mas ainda tem muito que evoluir.
P5.V3.1 – P2HES#02	Têm que evoluir ao nível dos mecanismos de autenticação, e ter uma política de registo das tarefas (*logs*) bastante forte. Quanto mais pessoais tiverem acesso à informação, quanto mais alargamos o leque maior a probabilidade de encontrar vulnerabilidades ou de formas de acesso incorretas. É necessário que se consiga rastrear o acesso aos dados a nível local, mas se os dados passam para um outro sistema, estes sistemas de *account* devem obrigatoriamente também permitir rastrear estes dados. Tem que haver uma evolução destes sistemas para que eles comecem também a partilhar informação de *logs*. Têm esta obrigatoriedade, caso contrário poderão existir

	aqui muitas falhas. Se não houver uma troca de informação, uma segunda validação, a um nível superior, poderá haver muitas falhas, e graves. Dentro do meu sistema eu sei quem são os meus utilizadores. Tenho mecanismos seguros de autenticação. Tenho políticas de proteção muito fortes dentro da autenticação. Agora se eu agarro num conjunto de dados clínicos e os transporto para um outro sistema, perco a noção de como é que estes dados vão ser utilizados e por quem. Estes sistemas de *account* têm que de uma forma transversal acompanhar os dados.
P5.V3.1 – P2HES#03	Nós tivemos que baixar um pouco a segurança nos nossos sistemas de *account*. As regras existentes estavam a dar grandes problemas aos utilizadores. Em relação ao que utilizador faz, temos aplicações que registam tudo o que utilizador faz, outras não tem um nível de detalhe elevado. É muito importante saber com detalhe em que dados o utilizador "mexeu". Já fizemos melhoramentos neste sentido. Temos estado a melhorar o historial do utilizador. Se houver uma falha esta informação é vial, para identificar quem falhou. Quando passamos dados para um outro sistema de outra instituição era útil saber onde é que estão esses dados. É necessário rastrear. Saber quem é que no outro sistema acedeu e alterou os dados.

P5.V4.1

P5.V4.1 – P1ULSNA#01	Numa fase de maturação deste processo seria o caminho para a excelência. Seria a forma de garantir que todos estariam a trabalhar da mesma forma. A certificação aumentaria a confiança entre as organizações, ao nível da partilha de informação, ao nível do conteúdo da informação não. Na relação do utente (titular dos dados) e dados que estes ainda estão pouco sensibilizados, o efeito seria diminuto
P5.V4.1 – P2ULSNA#02	Seria vantajosa uma certificação externa para a questão da proteção dos dados, que segue as boas práticas, agora por onde devemos começar esta certificação não tenho bem ideia. Aumentaria a confiança entre as organizações participantes e os utentes e também com outras organizações.
P5.V4.1 – P2ULSNA#03	A certificação significa que o serviço está pronto para. Esta certificação seria uma mais-valia, uma garantia à existência de menos falhas na segurança dos dados. A curto prazo é complicado afirmar que os utentes olhariam para a instituição de uma forma diferente para este tido de situações. A longo prazo o resultado será positivo.
P5.V4.1 – P4ULSNA#06	Sou um adapto de aumentarmos, não só a qualidade dos serviços, mas também aquilo que pode contribuir para o bem-estar dos cidadãos, da confiança que os cidadãos eventualmente depositam na organização, em que têm de confiar uma série de elementos. Efetivamente não é fácil lidar com os problemas da saúde, como em casos de doença em que a pessoa não é bem aceite pela sociedade. Penso que, se a contribuição for no sentido de aumentar a confiança do cidadão, e este saber que a instituição não esta a violar aquilo que são os princípios sobre o tratamento dos seus dados, a certificação é naturalmente muito importante. Agora deixe-me acrescentar, em Portugal, não conheço nenhum serviço que nesta perspetiva já esteja certificado, nem conheço

	entidades que desenvolvam certificação neste sentido. No sector privado, a questão da certificação surge como fazendo parte de uma estratégia comercial, o que não acontece no sector público. Para o domínio com a PDS, sem dúvida que aumentaria o nível de confiança. Vejo isto não só em virtude da segurança de utilização. A certificação implica um processo que é contínuo, que permite definir patamares de evolução. Já temos vários serviços certificados e que são auditados continuamente, senão perde-se a qualidade desejada. A mais recente foi uma auditoria à robustez dos sistemas de informação. A confiança e a própria segurança do utente saem beneficiadas, e temos que continuar a trabalhar neste sentido, dada a nossa responsabilidade social.
P5.V4.1 – P1USF#01	Sim faz sentido a certificação das organizações, trazendo maior confiança na empresa que está prestar aquele serviço. É diferente ser uma empresa certificada, desde que a certificação seja completamente séria. Uma das minhas maiores preocupações está relacionada com o problema associado ao facto de as organizações estarem cada vez mais a partilhar dados, a transportar mais dados entre bases de dados. Creio que a certificação por um lado, iria ajudar a um maior rigor. Quem estava a ser auditado a este nível sabia que aquela empresa sendo certificada, tendo um certo nível de confiança, sabia o que estava a fazer. Gerava-se uma maior confiança entre as organizações. Se as organizações souberem que vão ter o apoio de uma empresa certificadora isenta, que vai fazer um trabalho responsável, de uma forma rigorosa, que vão indicar o que está mal e o que está bem, então as organizações auditadas podem vir a trabalhar de uma forma diferente.
P5.V4.1 – P2USF#02	Acho que em todas as organizações temos enormes passos a dar ao nível da proteção de dados. Estamos a começar pelas infraestruturas, com regras que vão inclusive modificar a relação com os nossos parceiros, que têm que se adaptar constantemente. Ainda temos muitos passos para dar até que a privacidade seja logo contemplada na conceção dos sistemas.
P5.V4.1 – P4USF#05	Benefício para o doente ou para o profissional? Havendo esta cerificação trazia quer para o doente, quer para o profissional, uma certeza em que os seus dados não estão a ser expostos. Portanto a pessoa ficava mais tranquila, com maior confiança. Neste mundo global em que tudo é partilhado seria uma ferramenta essencial. Poderia também aumentar a confiança entre organizações. A PDS é sem dúvida uma ferramenta muito boa. Agora tem que haver é responsabilização dos profissionais que a utilizam. O objetivo da PDS é beneficiar o doente e não outros objetivos. O profissional tem que estar consciente disto.
P5.V4.1 – P1INEM#01	Uma certificação destas, pelo menos é uma forma de auditar. Auditar, dá sem dúvida uma garantia, que algo está definido, que há um conjunto de procedimentos que definem as normas de segurança. Mas, como tudo é falível. Por detrás disto tudo está sempre o ser humano. Pelo menos há uma normalização. Sabemos qual é o caminho. A confiança do cidadão aumentaria sabendo que uma instituição está certificada. Em relação à confiança entre organizações a certificação é um aspeto essencial à existência de partilha de dados. Apesar de deste momento nós não questionarmos a confiança em relação aos dados que partilhamos com outras instituições.

P5.V4.1 – P2INEM#03	Mais uma vez benificiária a visibilidade para a pessoa que vai fornecer os dados. Mais confiança. Se formos à relação entre os sistemas, de eu ter a garantir que são cumpridos os mesmos padrões que eu tenho internamente, penso que dará também mais confiança ao saber que aquela entidade tem esta certificação. Há uma maior confiança na troca de dados.
P5.V4.1 – P2INEM#04	A certificação seria vantajosa, traria benefícios, nomeadamente, logo de início, se a organização pretende sujeitar-se a uma sistema de certificação irá ter que fazer um trabalho prévio para fazer essa candidatura, e logo ai, se irão identificar muitas situações que provavelmente não serão as melhores, que podem ser corrigidas. Entraria num ciclo de melhoria. Seria importante à confiança entre as organizações na área da saúde. Alias penso que seria o trabalho mais visível, no trabalho que se fizesse nesse sentido.
P5.V4.1 – P2INEM#09	A certificação das organizações em matéria de proteção de dados seria sem dúvida benéfica, pelo facto de os cidadãos encararem as organizações com outra confiança. Apesar de em termos práticos poder haver algum exagero na sua implementação, promoveria sem dúvida uma maior confiança, mesmo entre organizações, pelas mesmas razões.
P5.V4.1 – P2INEM#10	Para mim sempre foi mais importante que as coisas existam e funcionem. A certificação é sempre importante. Hoje em dia está na moda, poder estar certificado. A grande vantagem da certificação é a garantia de aquilo está a ser cumprido. E neste sentido faz todo o sentido que ela exista. Para garantir a certificação vou ter que garantir conformidade com todas as normas existentes.
P5.V4.1 – P4INEM#08	É um caminho que temos que seguir, e é um caminho que o INEM quer seguir. Cada vez mais nós estamos dependentes de fornecedores externos de aplicações, e estes já têm como requisito nos seus produtos e serviços, este nível certificação da segurança. O facto, das instituições terem uma gestão das aplicações e das bases de dados muito dispare, ou seja, algo muito complexo, apesar de temos operadores no mercado com grande nível de fiabilidade e compromisso nesta área, com bases de dados internas, com desenvolvimento interno, muito "caseiras", muito adaptadas à realidade para responder às necessidades dos utilizadores, mais do que a necessidades mais abrangentes, torna este processo mais complexo. Porque para tornar este desenvolvimento interno possível de ser certificado, tenho que preencher um conjunto de requisitos, que tornaria ou poria em causa às vezes a sua própria existência. Um efeito prático, num processo de implementação da melhoria continua, é o aumento da segurança e da confiança. Não tenho a menor dúvida, e não tenho dúvida que seja o caminho. O problema é como é que se chega até lá! Há uma abordagem que é – para o normativo existe atualmente, para as exigências que existem atualmente, qual é o nível de execução? Isto seria o primeiro passo. Quantas bases de dados, as instituições cumpriram com os requisitos de acordo com o normativo legal? Quais foram submetidas à CNPD? Quais os processos submetidos à CNPD? Que recomendações foram promoveram alterações? Depois de autorizadas, foram alteradas e de novo avaliadas? Este será o primeiro diagnóstico.
P5.V4.1 – P1HFF#01	Quanto à segurança não creio que os sistemas tenham por base, políticas de segurança. A segurança é uma coisa que "custa" muito. Qualquer assunto no domínio da segurança, colocado a um administrador, se este não estiver focado na continuidade do negócio, se não tiver impacto na continuidade do negócio, ou até ao contrário, se a segurança que eu quero implementar, me obrigar a estrangular a minha continuidade do negócio, não se quer o mecanismo de segurança. A segurança custa muito – custo esforço, custa organização, custa muito dinheiro.

	Ao nível da administração eles não estão muito sensíveis a isto. Às questões da segurança. Agora a segurança dá sem dúvida mais conforto, mais notoriedade. Estou mais descansado, e posso promover junto da concorrência as minhas soluções. Em relação à evolução de uma certificação neste domínio a minha opinião é sim e não. Se eu penso logo à partida numa certificação os projetos podem morrer. Para eu certificar eu tenho que criar um âmbito. Tem que se circunscrever muito bem o âmbito para a certificação. E isto vai deixar algumas coisas de fora. O ecossistema é muito complexo. Eu acho que deveríamos apontar para a certificação, mas não de uma forma explícita. Devemos apontar para a certificação mas de uma forma discreta. Devemos apontar para a certificação, mas preocupados com as boas práticas. Cada organização tem a sua forma de trabalhar. Veja-se o caso do ITIL, em que algumas empresas apostam em introduzir o ITIL nos hospitais. Umas estão focadas em cumprir (em fazer o que precisam) e outras estão focadas em certificar. A certificação deve resultar de uma boa prática. Se eu conseguir um bom nível de implementação, aí posso pensar em partir para a certificação. A certificação deve ser vista mais como a garantia do funcionamento correto da proteção de dados, mas não deve ser divulgada. O custo associado e a complexidade são dois riscos para um processo desta natureza. Permitira aumentar um nível de confiança mas se se conseguir circunscrever o seu âmbito. Na minha opinião deveria haver mais monotorização destas questões (por parte da SPMS, do ministério) em prol de uma certificação. Seria essencial.
P5.V4.1 – P2HFF#02	A certificação é muito importante. Vai aumentar a preocupação das pessoas sobre a privacidade dos dados. No caso da PDS, aumentaria o nível de segurança e de confiança em relação à colaboração.
P5.V4.1 – P2HFF#03	Pode ser um caminho, mas a certificação per si, normalmente está agarrada a qualquer mais-valia para a organização. Se for só o bem comum ela não vai acontecer, ou muito dificilmente acontecerá. Se for porque é um objetivo institucional, imposto pela tutela, induz de facto à atenção das pessoas. Por exemplo, um processo de acreditação é um processo que vai dar muito trabalho, em que as pessoas além de prestarem cuidados e registarem a informação ainda vão ter que se preocupar com um conjunto de processos associados à qualidade dessa informação. Processos que têm a ver com a acreditação dessa atividade, que é paralelo com tudo o que já fazem. Ao nível do ministério da saúde, havendo um conjunto de regras, é fácil ao ministério da saúde proceder a esta certificação. Não é garantidamente um selo de qualidade nesta matéria, quando eu vejo outras acreditações, supostamente transversais, e em que acaba-se por certo tipo de situações que não estarem acauteladas pelo facto de eu estar acreditado. E eu vejo isso em áreas em que acreditava que a acreditação deveria dar essa garantia. Acabo por ver que em muitos aspetos ou a acreditação é imatura, e portanto muito filosófica, ou vai a um certo nível mas depois na prática não induz a diferença, não induz à alteração dos processos que deveria fazer.
P5.V4.1 – P4HFF#05	A privacidade será um caminho a seguir. Os processos de certificação, acreditação, obrigam antes de mais as organizações a pensarem, a discutirem o problema, e depois a implementarem a melhor solução. Estes processos têm a vantagem de colocar todas as estruturas de uma organização, neste caso num hospital, a conversar, a definir processos comuns, procedimentos comuns, de acordo com legislação, normas, melhores práticas caso existem. É uma garantia, não é um seguro.
P5.V4.1 – P1SPMS#02	A questão da certificação pode ser interessante. Uma certificação seria uma forma de saber que foi implementada uma política de

	privacidade, mas também depois ir auditando. Isto porque as certificações não são eternas. Através de auditorias percebe-se se algo está mesmo a ser implementado, e se existe a necessidade de fazer alguma revisão, alguma melhoria. Poderia ser uma forma de atrair entidades externas para a questão da proteção de dados. Teria de ser sempre alguém do exterior a certificar. Poderia não ser necessariamente uma empresa privada. Face à existência de *standard* consegue-se determinar se as instituições estão ou não de acordo com os requisitos. Havendo um *standard* seria uma vantagem. Quando se olha para um sistema certificado, tem a tendência a ter maior credibilidade. Seria mais por aí. No caso do ministério da saúde, não podemos estar a dar prioridade a uns e menos a outros, por terem um selo de certificado. Agora se me disser que em relação ao setor privado, e se nós obrigarmos a um certificado e ter politicas implementadas, nós desconfiamos mais. Desconfia-se mais do privado do que do setor público. Pode existir uma relação direta entre a questão da certificação e a confiança entre instituições. Alguém que seja externo e diga através de uma auditoria, que os processos estão bem implementados, que existem políticas implementadas devidamente, é uma segurança para quem está a ter um cenário de interoperabilidade ou outro. Confiamos um pouco mais por ter esse selo de certificação. 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.
P5.V4.1 – P2SPMS#03	O cumprimento das boas práticas na área da segurança já seria importante. Ter uma certificação e um cumprimento total não é uma tarefa fácil. É uma tarefa até bastante difícil. Que exige uma certa disciplina nas organizações. Este nível de exigência levaria a maioria das organizações a abandonar um projeto desta natureza. Caminhando-se neste sentido, e no contexto da partilha de dados através da PDS, uma certificação destas aumentaria a confiança entre as instituições. É necessário definir a que nível vai a certificação. Se for só de infraestruturas eu diria que não é suficiente. Tem que ser mais transversal e focada nos dados, perceber se aquilo que fazemos com os dados está de acordo com as regras definidas. Ajudaria certamente o processo de confiança.
P5.V4.1 – P2SPMS#04	A certificação pode ser um caminho a seguir. Tanto a certificação da proteção de dados como dos próprios sistemas. Os próprios sistemas muitas vezes não estão certificados. É um domínio que tem que se considerar no futuro. Havendo uma aposta na certificação há sem dúvida um aumento na confiança entre instituições em matéria de partilha de dados.
P5.V4.1 – P4SPMS#05	Certificar as práticas [de proteção de dados] ou as pessoas? A maior parte dos profissionais de IT não tem a formação adequada [em proteção de dados]. Esta certificação para a proteção de dados tem que certificar as práticas das pessoas. E para certificar as práticas das pessoas, têm que certificar as competências técnicas dessas pessoas. Se as pessoas não sabem fazer uma *query*, então não há *firewall* suficiente para proteger os dados! Acredito na certificação. É sempre bom a opinião externa sobre aquelas práticas e aqueles processos. Só que a proteção de dados depende de camadas, físicas obviamente, logicas [como é que são programados], e comportamentais. Poderia criar um ambiente mais seguro, mas tem que se certificar as pessoas. Fizeram ou não formação sobre privacidade e proteção dos dados? Estão ou não estão sensibilizados? Temos uma *workforce* que está preocupada com o assunto?

P5.V4.1 – P1HES#01	Uma das mais-valias será a confiança. As certificações acabam sempre por criar normas, regras, e conseguiríamos eventualmente garantir mais a privacidade da informação e transmitir segurança a todos nós, enquanto utentes. Se eu souber, enquanto utente, da existência desta certificação, não tinha colocado "não" na opção de consentimento da PDS. Certificando as instituições em matérias de proteção de dados, aumentaria a confiança na utilização da PDS.
P5.V4.1 – P2HES#02	Como benefícios, tínhamos uma certeza ou garantia que as politicas que são aplicadas numa organização são as mesmas, ou são no mínimo semelhantes às que estão a ser aplicadas noutras organizações. Portanto, se todas as organizações forem certificadas nós temos à partida um conjunto de garantias que nos tranquilizam, não só nós organização, como aos próprios utentes, ou outras pessoas visadas pela informação. sei que se uma instituição está certificada, os meus dados à partida estão garantidos, estarão sujeitos a um determinado número de critérios e de normas que me permitem estar mais descansado em relação à sua utilização. Esta certificação aumentava a confiança entre as organizações que participam por exemplo em projetos como a PDS.
P5.V4.1 – P2HES#03	A certificação é também um caminho para a proteção de dados. Para a certificação é necessário respeitar determinadas normas, determinados e protocolos. A grande vantagem da certificação e o aumento na proteção, uma vez que tem que se cumprir com normas e protocolos. Se os requisitos destas normas forem cumpridos, temos a garantia de uma maior proteção. Aumentava a confiança entre organizações quando se partilha dados para uma organização certificada. Tenho a garantia de que estes dados vão ser usados de forma correta.
P5.V4.1 – P4HES#06	Este caminho [da certificação] é fundamental. Mas não imagino como o podemos fazer com as ferramentas que temos atualmente. Já o conseguimos fazer ao nível a segurança, logo é possível caminharmos para uma certificação ao nível a proteção de dados. Tenho sempre alguma dificuldade em comparar o real com o virtual. Podemos até um diploma de certificação, mas temos as portas abertas. Isolando o nosso sistema de informação da PDS, tenho a noção que temos a solução mais avançada do país. Está implementada à vários anos, tem vindo a ser desenvolvida, e hoje em dia é uma ferramenta robusta, flexível, e muito apropriada aquilo a que nós fazemos com o registo clinico. Gostaria muito de a certificar internacionalmente. Contudo a grande fragilidade é a confidencialidade dos dados, uma vez que qualquer instituição do país entra nas nossas bases de dados e nós nem sabemos. Não acredito que nenhuma instituição internacional, se perceber como a PDS funciona, certifiquem os nossos sistemas. Não pode nascer a PDS e depois nascerem os controlos de privacidade. Nos temos um hospital que é o maior empregador do concelho, onde trabalha uma grande parte da população ativa da cidade. Onde quase toda a gente que reside na cidade é familiar, vizinho ou amigo dum profissional desta instituição. E tenho muitas reclamações de doentes que souberam de dados clínicos de exames que lhes foram pedidos aqui no hospital pelo vizinho. Porque a pessoa sabe que o vizinho foi fazer o exame e vai ao sistema e vê qual o resultado do exame, e anuncia à pessoa os resultados. Percebo que está concentrado nos dados de uma forma globalizada. A minha preocupação são os dados individuais. E há dois tipos de dados registados no hospital: dados clínicos e dados pessoais. Nós no hospital não registamos apenas dados clínicos. Na nossa prática clinica, também registamos dados pessoais. Os dados pessoais são relevantes para a parte clinica. Neste caso dados sobre a sua atividade profissional, social, sobre os seus contatos sexuais, doenças anteriores, hábitos, vícios, sobre uma série de coisas que tem a ver com a intimidade de cada um. Isto faz parte dos registos clínicos. E ter esta informação toda exposta, para quem a quiser consultar, através da PDS, vindo de onde vier, acho que não faz sentido.

	Dados administrativos preocupam-me menos.

2. *Data Reduction*

P5.V1.1	**Qual o contributo de um programa de responsabilidade. É uma ferramenta operacional necessária?** Compreender qual a importância atribuída aos programas de responsabilidade e averiguar se estes já são uma prática.	**Que partes podem desenvolver um programa de responsabilidade** Quem deve coordenar este processo e convocar as partes da organização interessadas no desenvolvimento de um programa de proteção da privacidade dos dados.
Padrão encontrado Utilidade/útil/confiança Diretrizes Proactiva Nível executivo/tutela Equipa multidisciplinar Iniciativa conjunta	"Poder pode, mas é um caminho complicado de seguir. Tem tudo a ver com uma questão cultural." (P5.V1.1 – P1ULSNA#01)	"Este é um processo que deve partir sempre da própria tutela, envolvendo todos os profissionais, numa equipa multidisciplinar, e de diversas instituições." (P5.V1.1 – P1ULSNA#01)
	"Se for feito a nível local não, se for feito a nível nacional penso que sim." (P5.V1.1 – P2ULSNA#02)	"A elaboração de políticas de privacidade com base na experiência de múltiplos locais facilita que a mensagem chegue a todos os envolvidos." (P5.V1.1 – P1ULSNA#01)
	"Pode contribuir, aliás contribuí." (P5.V1.1 – P2ULSNA#03)	"Um programa de responsabilidade tem que ser muito abrangente, para todas as organizações, devendo abranger conselhos de administração, conselhos de ética, sendo que estas questões ficam muito aquém dos conhecimentos que as comissões de ética possuem. Estamos a falar de três grupos: administração, área clinica, e tecnologias de informação. " (P5.V1.1 – P2ULSNA#02)
	"Penso que esta questão será necessariamente diferente no sistema público e no sistema privado. Penso que no privado será mais acutilante um programa de responsabilidade, porque muitas vezes as pessoas podem-se deixar levar pela estratégia comercial e esquecer eventualmente questões que salvaguardem a segurança e a confidencialidade dos dados. No público existe à partida uma cultura de respeito, ainda antes do surgimento dos sistemas tecnológicos." (P5.V1.1 – P4ULSNA#06)	"Internamente um processo destes deve iniciar-se na administração, como é óbvio, e a incluir a parte dos sistemas de informação." (P5.V1.1 – P2ULSNA#03)
	"Hoje em dia não existe nas instituições esta atitude de responsabilidade. Isto depende essencialmente da cultura das pessoas, e de saberem da responsabilidade dos lugares, que ocupam na sociedade. Estas regras ou responsabilização que fala poderia ser útil, mas poderá não ser decisiva." (P5.V1.1 – P1USF#01)	"Agora, existe aqui uma questão que é muito importante, que é a tutela - Ministério da Saúde, Administração Regional de Saúde. Esta pode definir esta ferramenta, dado que estão em causa múltiplas organizações. Tem que ser alguém que tenha a visão global destas questões, que apresente um poder efetivo. A tutela é muitas vezes a primeira a solicitar informação, a qual nós enviamos de forma anónima" (P5.V1.1 – P4ULSNA#06)
	"Poderia. Acho que faz todo o sentido este princípio. As normas são para cumprir. Temos que perceber sem dúvida, qual a nossa responsabilidade e por em prática medidas corretas." (P5.V1.1 – P2USF#02)	"Um processo desta natureza deve iniciar sempre na tutela, sempre o ministério da saúde a definir quais são as regras, as obrigações, os direitos. A partir daqui deve ser implementado junto dos profissionais responsáveis." (P5.V1.1 – P1USF#01)
	"Sim, vindo de cima, que obrigue a que certos itens sejam privados." (P5.V1.1 – P4USF#05)	"A administração central deve desenvolver este princípio, […]. E dentro de cada centro de saúde existir alguém responsável por isto." (P5.V1.1 – P4USF#05)
	"Nitidamente sim. Este terá que ser o caminho." (P5.V1.1 – P1INEM#01)	"O principal *sponsor*, digamos que deveria ser a direção, e depois claro delegar depois em outros responsáveis, até para que a política fosse efetivamente tida como um objetivo estratégico da organização." (P5.V1.1 – P1INEM#01)
	"Um programa destes poderia apresentar as principais diretrizes, que mais parte, poderiam ser materializadas em medidas e políticas de privacidade." (P5.V1.1 – P1INEM#01)	"Para o contexto de partilha de dados com outras instituições, o ministério da saúde, à semelhança de outros projetos, é fundamental para se integrar esta visão […]"(P5.V1.1 – P1INEM#01)
	"Tem que ser por aqui. O que infelizmente se vê na maior parte dos sítios não é uma pro-atividade, mas sim uma reação por imposição. Só quando são impostas regras é que se atua – se tem que ser vamos cumprir. Se conseguirmos alterar este paradigma seria vantajoso." (P5.V1.1 – P2INEM#03)	"Mas isto sempre integrado com aquilo que é o contexto de colaboração. Assim até o próprio ministério, saberia de uma forma transversal quais os princípios a serem aplicados." (P5.V1.1 – P1INEM#01)
	"Havendo diretrizes a este nível começa a adaptar-se todos os processos que existem, de modo a fazer cumprir estas ordens." (P5.V1.1 – P2INEM#03)	"Mas se ao nível da gestão de topo existir sensibilidade para tal, internamente
	"Pode ser um mecanismo útil, claro que sim." (P5.V1.1 – P2INEM#04)	
	"Deveria haver uma atitude proactiva em matérias de proteção de dados. As organizações são mais proactivas em questões de segurança." (P5.V1.1 – P2INEM#09)	

	“Não podemos esperar que as coisas aconteçam para depois a seguir remediar. Uma coisa é falar em teoria, outra coisa é a prática de proteção.” (P5.V1.1 – P2INEM#09)	numa organização, consegue-se ativar este princípio.” (P5.V1.1 – P2INEM#03)
	“Eu acho que sim. Nós temos, não sendo das melhores, algumas medidas ativas, quanto mais não seja para defesa interna dos funcionários e dos próprios utentes. Os processos de certificação em curso, são o exemplo de uma atitude pró-ativa.” (P5.V1.1 – P2INEM#10)	“Um processo destes teria de ser iniciado por um conjunto alargado de pessoas ligadas a diferentes atividades, em que nós (técnicos) estaríamos envolvidos.” P5.V1.1 – P2INEM#04
	“Sim, pode contribuir para sair da teoria. [...] Resumindo este princípio da responsabilidade pode funcionar como um catalisador para estas matérias.” (P5.V1.1 – P4INEM#08)	“Pode ser complicado em serem os gestores a tomarem a iniciativa, dado que a sua atividade em cada organismo é algo efémera. Um departamento de planeamento por exemplo, permitiria desenvolver esta questão de uma forma mais continua.” P5.V1.1 – P2INEM#04
	“Só faz sentido pensar em privacidade e segurança se eu tiver elementos ativos (informação, um computador, uma pessoa, um software). Ou seja, a importância de termos uma matriz de afectação de responsabilidades. E isto existe muito pouco.” (P5.V1.1 – P1HFF#01)	“Tem que ser uma iniciativa conjunta de todas as organizações para dar resultado. Senão pode vir a ser um esforço inglório.” P5.V1.1 – P2INEM#04
	“Esta atitude por parte das organizações permitiria passar para fora uma mensagem de confiança.” (P5.V1.1 – P2HFF#02)	“Todas as organizações que partilham dados devem participar ou iniciar um processo desta natureza. Tem que ser uma iniciativa conjunta, um compromisso conjunto, forçosamente. Internamente a sua implementação depende de decisões do topo das organizações.” (P5.V1.1 – P2INEM#10)
	“Eventualmente sim.” (P5.V1.1 – P2HFF#03)	“Agora se houver uma diretiva a sensibilizar para este princípio, este é interoperável entre organizações.” (P5.V1.1 – P1HFF#01)
	“Nos dias de hoje a privacidade é uma questão tão técnica como de gestão.” (P5.V1.1 – P4HFF#05)	“Isto só faz sentido se envolver todas as organizações. Promove mais a colaboração entre as instituições com base nas suas experiências.” (P5.V1.1 – P2HFF#02)
	“O demonstrar para o exterior que existe por parte da organização uma responsabilidade em matéria de proteção de dados é sem dúvida uma função de gestão, uma orientação estratégica.” (P5.V1.1 – P4HFF#05)	“Deveria ser desencadeado ao nível do ministério, deveria haver uma obrigação, uma portaria, uma recomendação para que em todas as instituições seja criado um gabinete que se preocupasse com este tipo de questões e que incluísse várias valências incluindo o gabinete jurídico, direções clinicas, responsáveis pelos sistemas de informação e responsáveis administrativos.” (P5.V1.1 – P2HFF#02)
	“Segundo a nossa experiência, muitas das instituições só atuam por obrigação. Infelizmente algumas são aconselhadas a implementar determinadas políticas, mas alegam que não têm o tempo para o fazer, que têm outras prioridades.” (P5.V1.1 – P1SPMS#02)	“Pode ser um grupo que seja criado no seio da administração central que depois em colaboração com quem está no terreno possa aqui redigir um conjunto de normas que depois possam ser implementadas nos diferentes sistemas hospitalares.” (P5.V1.1 – P2HFF#03)
	“É difícil, mas pode ajudar. É um bom princípio. Não é fácil muitas vezes perceber quem é o responsável. Quem é o responsável pelos dados. Hoje em dia é algo que é muito claro.” (P5.V1.1 – P2SPMS#03)	“Este tema tem que ser colocado sempre de cima para baixo. Nunca um hospital se vai preocupar com isso e ativar o princípio da responsabilidade.” (P5.V1.1 – P2HFF#03)
	“[...] é intenção nossa fomentar este principio. Ainda assim existiriam enormes dificuldades operacionais para implementar esta intenção, mais questões organizacionais do que técnicas, de formação das próprias pessoas.” (P5.V1.1 – P2SPMS#03)	“[...] tem que existir algum tipo de indicador para medir a qualidade, a exigência, a maturidade, de forma a ser possível mensurar se um hospital está de facto a pôr em prática ou não as medidas ao nível da privacidade.” (P5.V1.1 – P2HFF#03)
	“[...] acho que este princípio poderia ter um efeito prático positivo. Olhar para aquilo que é a legislação, perceber que implicação prática tem, e começar a implementar algumas medidas, pode ser um 1º passo importante.” (P5.V1.1 – P2SPMS#04)	“Ninguém melhor que o nível executivo para colocar o princípio da responsabilidade em prática. Mas compete à área técnica a sua execução e garantia do cumprimento deste princípio.” (P5.V1.1 – P4HFF#05)
	“Este princípio não tem que ser ativado, ele já lá está. Se é exercido ou não, ou se é transformado num componente relevante para o negócio, é diferente.” (P5.V1.1 – P4SPMS#05)	“Acredito que havendo um despacho, uma regulamentação, que obrigue a essa implementação [do princípio da responsabilidade] pode ser o passo essencial para que se concretize.” (P5.V1.1 – P1SPMS#02)
	“Um individuo em que a sua privacidade seja comprometida, fica “doente” na sua esfera social. Portanto como entidade de saúde, muito antes da lei de proteção dos dados, sempre houve a preocupação de cuidar dos dados.” (P5.V1.1 – P4SPMS#05)	“Deveria começar pelo topo das instituições, ser precedido por quem toma a decisão. Depois estamos da falar de sistemas de informação, os hospitais têm os seus sistemas de informação, e o seu representante poderia iniciar o processo a este nível, e depois escalando. Obviamente teria de ser criada a
	“Estamos a falar de medidas para garantir que a informação é utilizada de	

	forma segura e por quem a deve utilizar. Nós já trabalhamos um pouco no sentido do princípio da responsabilidade, até porque já temos vários exemplos de coisas que nós já fazemos para tentar garantir este princípio de alguma forma. Poderíamos fazer sim, nós e toda a gente, mais ações de sensibilização." (P5.V1.1 – P1HES#01)	condição para passar essa informação até aos profissionais." (P5.V1.1 – P1SPMS#02)
	Faz todo o sentido e é importante este princípio. Acho que as pessoas estão pouco sensibilizadas para o nível da proteção de dados. Não se preocupam muito quem tem acesso aos dados e sobre que condições. Não deveria ser assim, as pessoas têm que ter responsabilidade a este nível." (P5.V1.1 – P2HES#02)	"Uma diretiva nacional poderia iniciar este processo a nível nacional, tanto para o setor público como privado, que normalmente passa sempre ao lado. Poderíamos depois esbarrar com uma falta de preparação das organizações para estas questões." (P5.V1.1 – P1SPMS#02)
	"Este é um princípio que deveria já estar ativado. Seria um caminho para por em prática as questões da proteção e dados. Assim quando chegar a legislação já tínhamos algum conhecimento que nos permite adaptar com mais facilidade." (P5.V1.1 – P2HES#03)	"Seria necessário uma auditoria para perceber se está a ser implementado ou não, se existem dificuldades a implementar-se as medidas [...]" (P5.V1.1 – P1SPMS#02)
	"Deveria haver grandes diretrizes ao nível da proteção de dados uma vez que as aplicações atuais não garantem a segurança da informação."	"Só depende da boa prática de gestão. Já hoje é melhor para uma entidade gerir bem os dados, do que gerir mal." (P5.V1.1 – P4SPMS#05)
	"E deve haver uma atitude de responsabilidade [...]"	"A dinamização de um programa desta natureza depende para quem é dirigido. Se for para falar com médicos deve ser dirigido por um médico. As pessoas ouvem melhor os seus pares, do que se um responsável pela informática lhes disser quais as políticas a implementar, e a forma de as implementar." (P5.V1.1 – P1HES#01)
	"Poderá haver um alinhamento dos grandes princípios de privacidade entre instituições. Um compromisso entre instituições a nível nacional para com a proteção e dados." (P5.V1.1 – P4HES#06)	"Em qualquer um destes temas, a segurança, a privacidade, a política de responsabilidade, faz todos o sentido iniciar na gestão de topo, não tenho nenhuma dúvida sobre isto, mas depois encontrar os *players* certos dentro de cada grupo profissional que transmitam aos seus pares qual é que é caminho, e as mais-valias daquele caminho." (P5.V1.1 – P1HES#01)
	"É sempre importante fazer a monitorização e procurar avaliar dos riscos, e tentar perceber o que é que pode falhar." (P5.V2.2 – P2HES#03)	"Um programa de responsabilidade desta natureza, que contemplasse um conjunto de medidas obrigatórias, medidas gerais que permitisse às pessoas perceber aquilo que é a proteção de dados e a importância da sua privacidade, teria que vir do topo da instituição, do nível da administração, em colaboração com os responsáveis pelos sistemas de informação, gabinete jurídico, e outros responsáveis." (P5.V1.1 – P2HES#02)

P5.V2.1	**A análise de conformidade pode ser aplicada à privacidade dos dados?** À semelhança da prática regular da análise da conformidade das medidas de segurança, a privacidade dos dados deve ser incluídas nesta cultura de análise .	**De que forma um programa regular de análise de conformidade pode influenciar a privacidade dos dados.** É uma ferramenta de análise da eficácia das medidas de proteção desenhadas. Um meio de melhoria contínua.
Padrão encontrado Ferramenta [aplicável à privacidade dos dados] Análise continua Auditoria/auditar	"Antes de existir algo do ponto de vista técnico têm que existir em papel um conjunto de regras, definidas com base na legislação portuguesa, analisando o que é possível e exequível dentro deste tipo de instituição realizar. Uma equipa pode depois ser criada para analisar e avaliar os diferentes processos, ou processos escolhidos aleatoriamente." (P5.V2.1 – P2ULSNA#02)	"[…] esta análise pode ser uma melhoria para a organização, salvaguardando outros eventos que eventualmente possam questionar a proteção." (P5.V2.1 – P4ULSNA#06)
	"Com a segurança é possível testar a sua conformidade. Na privacidade dos dados esta também pode ser testada, simulando situações." (P5.V2.1 – P2ULSNA#03)	"É importante perceber se as nossas ferramentas, processos estão de acordo com a legislação." (P5.V2.1 – P2USF#02)
	"É possível, e desejável, fazer esta análise contínua de conformidade." (P5.V2.1 – P4ULSNA#06)	"Saber se está a ser cumprido certas medidas." (P5.V2.1 – P4USF#05)
	"Faz todo o sentido que a análise de conformidade seja contínua." (P5.V2.1 – P2USF#02)	"[…] verificar se está de acordo com a legislação, regulamentos ao nível interno. Desvios vão acontecer sempre, ou são passíveis de acontecer, dai a necessidade de uma verificação regular." (P5.V2.1 – P2INEM#03)
	"Sim. Fazer auditorias é importante." (P5.V2.1 – P4USF#05)	"Permite-mos averiguar se a proteção de dados está de acordo com as exigências existentes." (P5.V2.1 – P2INEM#04)
	"Sim, a análise de conformidade regular também deveria ser uma prática comum para a proteção de dados, […]" (P5.V2.1 – P2INEM#03)	"Permite analisar se estamos a cumprir com todas as boas práticas, ou não. Corrigimos o que está mal. Dentro do domínio dos dados deveria ser igual. Não deveríamos ficar limitados a infraestruturas, equipamentos. Em termos de dados esta análise é mais exigente." (P5.V2.1 – P2INEM#09)
	"Uma análise de conformidade à proteção de dados seria útil. É necessário mais monotorização. No fundo as soluções são implementadas e depois não são monitorizadas com a atenção devida." (P5.V2.1 – P2INEM#04)	"Só assim é que posso garantir a eficácia das medidas. Eu só consigo garantir a eficácia se reavaliar regularmente." (P5.V2.1 – P2INEM#10)
	"Sim a análise regular da conformidade da utilização de dados seria uma ferramenta fundamental." (P5.V2.1 – P2INEM#09)	"[…] tem que haver uma grande preocupação em sensibilizar as pessoas para esta área, tem que haver uma grande preocupação em utilizar ferramentas que permitam o diagnóstico e a rápida resolução das questões diárias, e depois passar para o nível de exigência ao nível do certificado de confiança." (P5.V2.1 – P4INEM#08)
	"Sim esta ferramenta faz todo o sentido - a análise da conformidade. Faz sentido regularmente fazer uma análise de conformidade das políticas de privacidade." (P5.V2.1 – P2INEM#10)	"O conhecimento de todos os processos de recolha e tratamento de dados é uma boa base de atuação. Juntando aquilo que é legislação estamos em condições de perceber se estamos ou não de acordo com a legislação de proteção de dados." (P5.V2.1 – P2HFF#02)
	"A análise da conformidade também se deveria adaptar ao nível da proteção de dados." (P5.V2.1 – P4INEM#08)	"[…] a monitorização da utilização de dados deve ser continua, assim como a implementação de medidas para termos essa garantia." (P5.V2.1 – P4HFF#05)
	"Em relação à proteção de dados, é viável, deveria existir também uma matriz de análise." (P5.V2.1 – P2HFF#02)	"Daí que seja passível de implementar uma análise de conformidade em relação à segurança dos dados. Em relação à privacidade dos mesmos penso ser mais complicado uma análise de conformidade." (P5.V2.1 – P2SPMS#03)
	"Esta análise regular da conformidade da proteção de dados depende de um guião, de um padrão, tal como já se faz para a segurança." (P5.V2.1 – P2HFF#02)	"Ferramentas para perceber se estamos a fazer um bom trabalho, em matéria de proteção e privacidade dos dados." (P5.V2.1 – P2SPMS#04)
	"Aquilo que é prática dominante na segurança de análise de conformidade. Tem de se movimentar para os dados." (P5.V2.1 – P2HFF#03)	"Se percebermos quais são os riscos em termos de informação, podemos depois verificar regularmente se estamos a conseguir eliminar o risco. Neste momento já estamos com várias iniciativas de auditoria relacionadas com a qualidade dos dados. O próximo passo vai ser sem dúvida a parte da proteção destes dados." (P5.V2.1 – P2SPMS#04)
	"Para a área de proteção, privacidade dos dados deveria haver à semelhança da segurança, uma análise de conformidade continua." (P5.V2.1 – P4HFF#05)	"A aplicação das normas ISO27001 por exemplo, que fala especificamente com
	"A análise de conformidade deveria ser uma ferramenta também aplicável à privacidade dos dados. Só com auditoria se consegue verificar se se cumpre." (P5.V2.1 – P2SPMS#03)	
	"Auditar-se regularmente aquilo que é a utilização dos dados, à semelhança da segurança seria vantajoso. Não temos ainda ferramentas para isso." (P5.V2.1 –	

	P2SPMS#04)	a componente de conformidade da segurança. A aplicação desta norma à gestão da informação não é fácil. A definição das medidas de proteção dos dados não é fácil." (P5.V2.1 – P2HES#02)
	"Em primeiro devem ter uma análise de segurança. Muitas instituições [na área da saúde] ainda não têm esta prática." (P5.V2.1 – P4SPMS#05)	"Verificar se os dados estão a ser utilizados de uma forma correta, se não existem erros na informação, se estes não foram adulterados. São necessárias ações preventivas." (P5.V2.1 – P2HES#03)
	"A análise de conformidade como ferramenta deveria também estar a ser aplicada à proteção de dados." (P5.V2.1 – P2HES#02)	"Devemos olhar para os sistemas com um acesso de uma forma controlada e não de uma forma totalmente aberta, caso contrário entramos num caos." (P5.V2.1 – P4HES#06)
	"Devíamos estar a adaptar esta análise de conformidade também aos dados." (P5.V2.1 – P2HES#03)	*"Pode permitir traçar mapas de tendência de acesso, determinadas utilizações específicas que não pensávamos existir. Este tipo de avaliação permitiria conhecer claramente que tipo de procura de informação ou dados é suspeita […]" (P5.V2.3 – P2ULSNA#02)*
	"Tal como olhamos para a criticidade dos sistemas informáticos deveríamos olhar também para a criticidade dos dados." (P5.V2.1 – P4HES#06)	*"A identificação de padrões seria importante, com base na identificação dos utilizadores, perceber com base numa linguagem de análise, que dados devem ser monitorizados." (P5.V2.3 – P2ULSNA#02)*
	"Nós não olhamos para os dados com a atenção que eles merecem." (P5.V2.2 – P2INEM#10)	

P5.V2.2	Que fatores são determinantes na definição do nível de exigência e periodicidade para um processo de análise
Padrão encontrado	"Apesar da importância da privacidade, não fazemos nada para a defender [...]" (P5.V2.2 – P2ULSNA#02)
Criticidade dos dados	"Tal como na segurança a criticidade é importante. É importante sempre que possível anonimizar o utente, protegendo assim o que está por detrás desse utente." (P5.V2.2 – P2ULSNA#02)
Exposição dos dados	"Através de uma análise periódica sobre transferências, sobre tudo aquilo que é feito de dentro para fora." (P5.V2.2 – P2ULSNA#03)
Risco	"A qualidade dos dados é determinante. Dados mais sensíveis obrigam a uma maior preocupação. O volume de dados tratados, não considero importante. Importante sim é se os dados são ou não críticos. Se conhecermos bem o cenário de utilização, o risco associado, poderemos prepararmo-nos melhor." (P5.V2.2 – P2USF#02)
	"A sensibilidade dos dados vai definir a prioridade." (P5.V2.2 – P2INEM#03)
	"Poderá ser a sensibilidade e exposição dos dados, a forma como poderão estar a ser utilizados. A sua maior ou menor confidencialidade obrigam a que se faça um controlo, assim como a sua maior ou menor exposição." (P5.V2.2 – P2INEM#04)
	"O conhecimento do ciclo de vida dos dados é importante. O facto de a sensibilidade dos dados ser mais crítica, como dados clínicos de hospitais, vai determinar o que é prioritário que termos de auditorias." (P5.V2.2 – P2INEM#09)
	"Onde temos informação pessoal, sensível, garantidamente tem que ser dada mais atenção." (P5.V2.2 – P2INEM#10)
	"Quando um processo é mais crítico, quando uma ferramenta é mais crítica é necessário uma maior atenção." (P5.V2.2 – P2INEM#10)
	"Tem a ver com a maturidade da instituição. Existem áreas onde os dados são mais sensíveis, o que implica que mais regularmente se faça esta análise de conformidade." (P5.V2.2 – P2HFF#02)
	"Com uma análise de risco, como já falamos, haveria um maior conhecimento sobre o risco de cada situação de utilização de dados e se houver uma área onde existe por exemplo uma maior intensidade de utilização de dados deve-se incidir com mais medidas." (P5.V2.2 – P2HFF#02)
	"Em relação aos dados se eu optar por uma política de análise de conformidade continua, e face à maturidade em que nós estamos, garantidamente a sensibilidade dos dados. Áreas críticas em relação à informação." (P5.V2.2 – P2HFF#03)
	"Toda a informação que tiver impacto, sendo que a informação é poderosa em termos económicos, que tem relação com seguradoras, com questões legais, tem que garantir que essa informação está mais protegida." (P5.V2.2 – P2HFF#03)
	"Agora no caso de um hospital tudo que é informação clinica, pura e dura, é crítica. Existe uma relação direta com a análise de risco." (P5.V2.2 – P2HFF#03)
	"Depende da dimensão do que estivermos a falar e do seu impacto. Depende muito do sistema em si, do tipo de dados que estamos a utilizar, da sua criticidade." (P5.V2.2 – P2SPMS#03)
	"Tem muito a ver com a análise do risco, é determinante. Depende muito daquilo que é o impacto do que é uma falha de privacidade sobre aquela informação." (P5.V2.2 – P2SPMS#03)
	"Onde existir informação mais critica, concordo que se devesse investir mais neste tipo de auditoria. Informação do domínio administrativo não é tão perigosa como informação do domínio clinico, em termos de privacidade." (P5.V2.2 – P2SPMS#04)
	"Onde tivermos dados mais sensíveis deveria haver uma maior proteção. Cenários de partilha de dados também deveriam ser auditados com mais frequência." (P5.V2.2 – P2SPMS#04)
	"Onde houver informação mais sensível, provavelmente tem que se analisar mais vezes a sua conformidade." (P5.V2.2 – P2HES#02)
	"Com informação mais critica, nomeadamente análises clinicas, deve ser analisada a sua conformidade com mais regularidade." (P5.V2.2 – P2HES#03)

P5.V2.3	São resultados a publicar? A publicação dos resultados deveria ser uma prática, funcionando como um "selo de qualidade".	Qual o efeito prático caso os resultados sejam tornados públicos. Quais os efeitos práticos imediatos, que podem surgir com a publicação dos resultados dos processos de análise de conformidade.
Padrão encontrado Impacto Confiança Garantias	"Claro." (P5.V2.3 – P2ULSNA#02)	"O tornar publica desta informação, cria do outro lado uma maior confiança no sistema de informação." (P5.V2.3 – P2ULSNA#02)
	"Eu acho que sim. Contudo esta publicação depende da necessidade de ter a certeza que temos assegurado estes procedimentos de conformidade. A certificação surge neste caminho." (P5.V2.3 – P2ULSNA#03)	"Uma mais-valia para a própria instituição, porque havendo resultados positivos, seriam benéficos para a instituição." (P5.V2.3 – P2ULSNA#03)
	"Sim sem dúvida, faz todo o sentido. Concordo com a publicação destes resultados." (P5.V2.3 – P2USF#02)	"Diga-mos que "alertar", seja a publicação boa ou má. Permite comunicar o que temos e onde não cumprimos. E se não cumprimos vamos ter que mudar. Acho que todas as organizações deveriam fazer isto, e definir objetivos neste domínio." (P5.V2.3 – P2USF#02)
	"Poderá ser vantajoso, à semelhança da segurança." (P5.V2.3 – P2INEM#03)	"Alem de aumentar a confiança entre as organizações, se estes dados são publicados não apenas internamente através das intranets, e são publicados no exterior, aumenta a confiança para os utentes, para o próprio cidadão." (P5.V2.3 – P2USF#02)
	"Era positivo [...]" (P5.V2.3 – P2INEM#04)	"Pode trazer mais descanso e garantias às pessoas ao fornecerem um conjunto de informação." (P5.V2.3 – P2INEM#03)
	Da mesma forma em que a certificação numa norma ISO dá confiança, da mesma forma a publicação desta análise poderia promover o mesmo." (P5.V2.3 – P2INEM#09)	"Entre as organizações poderia criar pontos de confiança, alias uma das coisas muito sensível entre as organizações é precisamente a desconfiança em relação à segurança, [...], mais da parte dos médicos, que se procuram defender em relação à exposição de determinada informação." (P5.V2.3 – P2INEM#04)
	Se esta constituir uma boa prática deve ser publicada. Caso contrário deverá ser utilizada esta informação para corrigir os problemas identificados." (P5.V2.3 – P2INEM#09)	"Agora quando não se cumpre, quando as coisas não correm bem é necessário assegurar que estamos mesmo a resolver." (P5.V2.3 – P2INEM#10)
	À semelhança do que já se faz com os testes de robustez para as infraestruturas, deveria pensar-se em algo semelhante para os dados, para a sua proteção." (P5.V2.3 – P2INEM#09)	"A publicação destes resultados aumenta a confiança que as pessoas podem dar a essa organização." (P5.V2.3 – P2HFF#02)
	"[...] estas questões devem ser sempre públicas. Não faz sentido esconder as coisas." (P5.V2.3 – P2INEM#10)	"A transparência é essencial à confiança na organização, e para que os próprios profissionais façam a sua própria auto validação da qualidade da informação." (P5.V2.3 – P2HFF#03)
	"Esta publicação pode ter um efeito positivo para a organização, faz todo o sentido." (P5.V2.3 – P2INEM#10)	"No caso de existir conformidade em relação a todos os requisitos externos, aqui a sua publicação poderia transmitir alguma confiança aos utilizadores externos, aos utentes do SNS. No caso da não conformidade poderia causar uma desconfiança." (P5.V2.3 – P2SPMS#03)
	"Tem que haver transparência. Se não houver transparência do que é que nos serve a privacidade?" (P5.V2.3 – P2HFF#02)	"As pessoas poderiam desta forma ficar mais conscientes deste problema. As pessoas hoje em dia nem se apercebem das consequências." (P5.V2.3 – P2SPMS#04)
	"Sim, demonstrar que estamos de acordo com um conjunto de requisitos. Num processo de qualidade, ou em processos de cumprimentos de indicadores, demonstrar o que fizemos é importante." (P5.V2.3 – P2HFF#03)	"Com a publicação dos resultados as pessoas podem ficar consciencializadas com o problema. Demonstrar que o que foi feito até aqui, não foi feito da melhor forma, e que se aplicarmos novas medidas iremos melhorar." (P5.V2.3 – P2HES#02)
	"Diria que por vezes pode não ser benéfica, porque pode criar algum alarmismo em quem desconhece o processo. [...]. Até para a opinião pública em geral conseguir perceber exatamente o que é aquela não conformidade e o que ela pode representar e qual é a probabilidade de ela acontecer." (P5.V2.3 – P2SPMS#03)	"Estando tudo bem desencadeia uma confiança em quem nos entrega os dados. [...] Deveria ser um requisito, as instituições provarem que cumprem com a legislação em relação à proteção de dados e à segurança." (P5.V2.3 – P2HES#03)
	"Acho importante a publicação deste tipo de análises e resultados em relação à proteção de dados." (P5.V2.3 – P2SPMS#04)	
	"Eu acho que a publicação destes resultados deve acontecer e deve ser vista num sentido pedagógico." (P5.V2.3 – P2HES#02)	
	"Devíamos estar a caminhar para "selos de garantia" ao nível da proteção e dados [...]" (P5.V2.3 – P2HES#02)	
	"É importante a publicação destes resultados. [...] Não sei se o termo correto será publicar, e não informar. Informar as instituições intervenientes sobre os pontos de falha, que desencadeiem uma ação." (P5.V2.3 – P2HES#03)	

P5.V3.1	Responsabilização sobre a utilização dos dados O registo e monitorização das ações realizadas sobre os dados são uma ferramenta fundamental à privacidade dos dados. Qual a preparação e compreensão atuais?	Qual a evolução desejável para os sistemas de registo das ações realizadas sobre os dados. Analisar de que forma esta evolução é essencial à privacidade dos dados. Analisar a relação com a questão da identidade digital.
Padrão encontrado Prova de evidência Prova de utilização	"A nossa experiência [...] em sistemas deste tipo é praticamente nula. A partilha de informação que existe vem do ministério da educação e acabamos por não estar cientes do que é partilhado, do que é divulgado." (P5.V3.1 – P2ULSNA#02)	"Para o contexto de colaboração este tratamento obrigatoriamente tem que ser mais exaustivo. Existe uma grande falha neste domínio." (P5.V3.1 – P2ULSNA#03)
	"Acima de tudo devem registar quem fez o quê. É importantíssimo o registo tanto para o bem como para o mal." (P5.V3.1 – P2ULSNA#03)	"Seria desejável uma maior interoperabilidade entre os sistemas de *account* das várias organizações." (P5.V3.1 – P2USF#02)
	"No nosso caso não existe uma observação periódica destes dados a nível local." (P5.V3.1 – P2ULSNA#03)	"Existem normas que têm que ser cumpridas. Temos que conseguir saber quem está a aceder aos dados, e isto é triado todos os dias." (P5.V3.1 – P2USF#02)
	"No domínio da saúde, já se consegue perceber quem acedeu e de onde acedeu aos dados. Em termos de privacidade é o início para se perceber que temos à disposição neste momento ferramentas que nos permitem pelo menos controlar o acesso às nossas aplicações, e se houver um problema nós conseguimos responder: nesse local, na hora tal, foi efetuada determinada tarefa." (P5.V3.1 – P2USF#02)	"Se queremos ter partilha de dados, estes sistemas têm que funcionar integrados. Eu consigo controlar os meus dados, mas fico preocupado quando os meus dados transitam para outros sistema, que eu não sei como vão ser tratados lá, e isto é um direito da organização, saber como estão a ser tratados os dados." (P5.V3.1 – P2INEM#03)
	"Estes sistemas são importantes para o contexto de partilha de dados. Só pelo facto de poder facilitar a partilha de dados, ao produzirem prova da utilização de dados, já são importantes." (P5.V3.1 – P2INEM#03)	"Se eu tenho requisitos de confidencialidade eu tenho que ter garantias que as outras organizações têm os mesmos padrões." (P5.V3.1 – P2INEM#03)
	"Em determinado tipo de utilizações é um pouco isso que nós já fazemos, não só para acautelar os dados, como também para percebermos se a utilização que estão a fazer dos sistemas é a correta ou não, e também para percebermos que quando há um erro, exatamente onde é que ele está a ser gerado." (P5.V3.1 – P2INEM#04)	"Com os dados a fluir cada vez mais entre sistemas, estes sistemas [*accountability*] têm que se adaptar. Eu perco o controlo sobre os dados. Idealmente estes sistemas [*accountability*] têm que começar a integrar-se uns com os outros, a partilhar informação, de modo a eu poder saber para os dados que saíram do meu sistema o que é que estão a fazer com eles." (P5.V3.1 – P2INEM#04)
	"O registo de todas as tarefas realizadas localmente ou remotamente são uma garantia de que os dados estão a ser utilizados de forma correta." (P5.V3.1 – P2HFF#02)	"Idealmente, os sistemas [de *accountability*] devem ser capazes de dialogar entre si." (P5.V3.1 – P2INEM#10)
	"Internamente já estamos no domínio dos sistemas de informação, a avaliar a qualidade dos dados que estão a ser registados. E esta avaliação da qualidade dos dados registados vai nos ajudar também muito em relação à privacidade." (P5.V3.1 – P2HFF#02)	"A partir do momento em que os dados passam para outro sistema, eu perco o "rasto" a estes dados. Tem que haver uma integração futura destes sistemas. Seria solução ideal." (P5.V3.1 – P2INEM#10)
	"Eles são muito a prova de evidência quanto à utilização dos serviços. Consigo já chegar aos dados, no que toca a prova de evidência, provar que um utilizador alterou e utilizou estes dados." (P5.V3.1 – P2HFF#03)	"Agora é importante perceber de forma granular o que se passou com a utilização dos dados." (P5.V3.1 – P2HFF#02)
	"Pela minha experiência o accountability é quase sempre realizado de uma forma isolada, com cada aplicação a fazer o seu registo." (P5.V3.1 – P2SPMS#03)	"Quando passamos dados para um outro sistema, perdemos o rasto a esses dados. Quando falamos em identidade digital, deveria ser possível que todos os dados fossem assinados com um certificado digital." (P5.V3.1 – P2HFF#02)
	"Disponibilizar esta informação ao utente era relevante. Ficaria a saber quem acedeu à sua informação." (P5.V3.1 – P2SPMS#03)	"É necessário que estes sistemas evoluam do controlo dos utilizadores e dos serviços para os dados. A malha de colaboração depende de mecanismos que obriguem a tecnologia a colaborar." (P5.V3.1 – P2HFF#02)
	"O *account* de sistema, em que é registado a entrada e saída de um utilizador é nitidamente insuficiente." (P5.V3.1 – P2SPMS#03)	"É difícil estes sistemas adaptarem-se aquilo que é cada vez mais a interoperabilidade entre organizações. O desafio é gigantesco. Porque nós não damos qualidade à informação, não atribuímos uma característica à informação, para a poder depois classificar e adequar. Simplesmente, nós enviamos a informação. E depois quando a informação vai para outro repositório, é o outro sistema que exerce o controlo, e que é diferente do meu. Isso é a realidade." (P5.V3.1 – P2HFF#03)
	"O básico é que estes sistemas registem a entrada e saída do profissional, e depois todas as tarefas que realizou têm de ficar registadas. [...] Quando	"Tem que haver uma interoperabilidade técnica a nível destes sistemas."

	falamos de informação de passa de uma base de dados de um sistema para outra base de dados de um outro sistema, perco o rastro aos dados. Não sabemos o que é feito com os dados do outro lado. No fundo a PDS já começa a rastrear a utilização dos dados a nível nacional, mas ainda tem muito que evoluir." (P5.V3.1 – P2SPMS#04)	(P5.V3.1 – P2HFF#03)
	"Quanto mais pessoais tiverem acesso à informação, quanto mais alargamos o leque maior a probabilidade de encontrar vulnerabilidades ou de formas de acesso incorretas." (P5.V3.1 – P2HES#02)	"A sua evolução deve contemplar pelo menos a informação sobre quem acede aos dados, quem os altera, quem os cria. Na maior parte dos sistemas não existe este conceito." (P5.V3.1 – P2SPMS#03)
	"Agora se eu agarro num conjunto de dados clínicos e os transporto para um outro sistema, perco a noção de como é que estes dados vão ser utilizados e por quem. Estes sistemas de *account* têm que de uma forma transversal acompanhar os dados." (P5.V3.1 – P2HES#02)	"Quando os dados passam para um outro sistema externo, deve ser evocado em que contextos estão a ser passados. Deveria existir em termos de histórico. Deveria ser sempre possível rastrear os dados, mesmo para lá do nosso sistema. Pelo menos o contexto em que eles passaram para o outro sistema." (P5.V3.1 – P2SPMS#03)
	"Em relação ao que utilizador faz, temos aplicações que registam tudo o que utilizador faz, outras não tem um nível de detalhe elevado." (P5.V3.1 – P2HES#03)	"Tem que se ir mais longe em que é necessário registar quem acedeu à minha informação e em que contexto. É necessário perceber qual é fluxo de negócio dos dados. É no fundo um registo baseado nos dados e não apenas nos utilizadores. Ainda não temos isto." (P5.V3.1 – P2SPMS#03)
		"Têm que evoluir ao nível dos mecanismos de autenticação, e ter uma política de registo das tarefas (*logs*) bastante forte." (P5.V3.1 – P2HES#02)
		"É necessário que se consiga rastrear o acesso aos dados a nível local, mas se os dados passam para um outro sistema, estes sistemas de *account* devem obrigatoriamente também permitir rastrear estes dados." (P5.V3.1 – P2HES#02)
		"Tem que haver uma evolução destes sistemas para que eles comecem também a partilhar informação de *logs*. Têm esta obrigatoriedade, caso contrário poderão existir aqui muitas falhas." (P5.V3.1 – P2HES#02)
		"Se houver uma falha esta informação é vital, para identificar quem falhou." (P5.V3.1 – P2HES#03)
		"Quando passamos dados para um outro sistema de outra instituição era útil saber onde é que estão esses dados. É necessário rastrear. Saber quem é que no outro sistema acedeu e alterou os dados." (P5.V3.1 – P2HES#03)

P5.V4.1	Benefícios que pode surgir com a certificação Qual o impacto de um esquema de certificação específico para a proteção de dados para a globalidade dos sistema de informação?	Impacto sobre o ambiente de colaboração. É uma ferramenta essencial à promoção de um ambiente de interoperabilidade confiável e seguro?
Padrão encontrado Garantia/mais-valia Confiança Complexo de implementar	"Numa fase de maturação deste processo seria o caminho para a excelência. Seria a forma de garantir que todos estariam a trabalhar da mesma forma." (P5.V4.1 – P1ULSNA#01)	"A certificação aumentaria a confiança entre as organizações, ao nível da partilha de informação, ao nível do conteúdo da informação não." (P5.V4.1 – P1ULSNA#01)
	"Seria vantajosa uma certificação externa para a questão da proteção dos dados [...]" (P5.V4.1 – P2ULSNA#02)	"Aumentaria a confiança entre as organizações participantes e os utentes e também com outras organizações." (P5.V4.1 – P2ULSNA#02)
	"Esta certificação seria uma mais-valia, uma garantia à existência de menos falhas na segurança dos dados." (P5.V4.1 – P2ULSNA#03)	"A curto prazo é complicado afirmar que os utentes olhariam para a instituição de uma forma diferente para este tido de situações. A longo prazo o resultado será positivo." (P5.V4.1 – P2ULSNA#03)
	"Penso que, se a contribuição for no sentido de aumentar a confiança do cidadão, e este saber que a instituição não esta a violar aquilo que são os princípios sobre o tratamento dos seus dados, a certificação é naturalmente muito importante." (P5.V4.1 – P4ULSNA#06)	"Para o domínio com a PDS, sem dúvida que aumentaria o nível de confiança. Vejo isto não só em virtude da segurança de utilização. A certificação implica um processo que é contínuo, que permite definir patamares de evolução." (P5.V4.1 – P4ULSNA#06)
	"Sim faz sentido a certificação das organizações [...]" (P5.V4.1 – P1USF#01)	"A confiança e a própria segurança do utente saem beneficiadas, e temos que continuar a trabalhar neste sentido, dada a nossa responsabilidade social." (P5.V4.1 – P4ULSNA#06)
	"Acho que em todas as organizações temos enormes passos a dar ao nível da proteção de dados. Estamos a começar pelas infraestruturas [...]" (P5.V4.1 – P2USF#02)	"Creio que a certificação por um lado, iria ajudar a um maior rigor. Quem estava a ser auditado a este nível sabia que aquela empresa sendo certificada, tendo um certo nível de confiança, sabia o que estava a fazer. Gerava-se uma maior confiança entre as organizações." (P5.V4.1 – P1USF#01)
	"Ainda temos muitos passos para dar até que a privacidade seja logo contemplada na conceção dos sistemas." (P5.V4.1 – P2USF#02)	"Neste mundo global em que tudo é partilhado seria uma ferramenta essencial. Poderia também aumentar a confiança entre organizações." (P5.V4.1 – P4USF#05)
	"Havendo esta cerificação trazia quer para o doente, quer para o profissional, uma certeza em que os seus dados não estão a ser expostos. Portanto a pessoa ficava mais tranquila, com maior confiança." (P5.V4.1 – P4USF#05)	"Em relação à confiança entre organizações a certificação é um aspeto essencial à existência de partilha de dados. Apesar de deste momento nós não questionarmos a confiança em relação aos dados que partilhamos com outras instituições." (P5.V4.1 – P1INEM#01)
	"Auditar, dá sem dúvida uma garantia, que algo está definido, que há um conjunto de procedimentos que definem as normas de segurança. Pelo menos há uma normalização. Sabemos qual é o caminho." (P5.V4.1 – P1INEM#01)	"Há uma maior confiança na troca de dados." (P5.V4.1 – P2INEM#03)
	"A certificação seria vantajosa, traria benefícios, [...]. Entraria num ciclo de melhoria." (P5.V4.1 – P2INEM#04)	"Seria importante à confiança entre as organizações na área da saúde. Alias penso que seria o trabalho mais visível [...]" (P5.V4.1 – P2INEM#04)
	"[...] seria sem dúvida benéfica, pelo facto de os cidadãos encararem as organizações com outra confiança." (P5.V4.1 – P2INEM#09)	"[...] promoveria sem dúvida uma maior confiança, mesmo entre organizações [...]" (P5.V4.1 – P2INEM#09)
	"A certificação é sempre importante. [...] A grande vantagem da certificação é a garantia de aquilo está a ser cumprido." (P5.V4.1 – P2INEM#10)	"Um efeito prático, num processo de implementação da melhoria continua, é o aumento da segurança e da confiança. Não tenho a menor dúvida, e não tenho dúvida que seja o caminho." (P5.V4.1 – P4INEM#08)
	"Para garantir a certificação vou ter que garantir conformidade com todas as normas existentes." (P5.V4.1 – P2INEM#10)	"Agora a segurança dá sem dúvida mais conforto, mais notoriedade. Estou mais descansado, e posso promover junto da concorrência as minhas soluções." (P5.V4.1 – P1HFF#01)
	"[...] com desenvolvimento interno, muito "caseiras", muito adaptadas à realidade para responder às necessidades dos utilizadores, mais do que a necessidades mais abrangentes, torna este processo mais complexo. Porque para tornar este desenvolvimento interno possível de ser certificado, tenho que preencher um conjunto de requisitos, que tornaria ou poria em causa às vezes a sua própria existência." (P5.V4.1 – P4INEM#08)	"Para eu certificar eu tenho que criar um âmbito. Tem que se circunscrever muito bem o âmbito para a certificação. E isto vai deixar algumas coisas de fora." (P5.V4.1 – P1HFF#01)
	"Qualquer assunto no domínio da segurança, colocado a um administrador, se este não estiver focado na continuidade do negócio, se não tiver impacto na continuidade do negócio, ou até ao contrário, se a segurança que eu quero implementar, me obrigar a estrangular a minha continuidade do negócio, não se quer o mecanismo de segurança." (P5.V4.1 – P1HFF#01)	"Permitira aumentar um nível de confiança mas se se conseguir circunscrever o seu âmbito. Na minha opinião deveria haver mais monotorização destas

	“O ecossistema é muito complexo. Eu acho que deveríamos apontar para a certificação, mas não de uma forma explícita. Devemos apontar para a certificação mas de uma forma discreta. Devemos apontar para a certificação, mas preocupados com as boas práticas.” (P5.V4.1 – P1HFF#01)
	“A certificação deve ser vista mais como a garantia do funcionamento correto da protecção de dados, mas não deve ser divulgada. O custo associado e a complexidade são dois riscos para um processo desta natureza.” (P5.V4.1 – P1HFF#01)
	“A certificação é muito importante.” (P5.V4.1 – P2HFF#02)
	“Pode ser um caminho, mas a certificação per si, normalmente está agarrada a qualquer mais-valia para a organização.” (P5.V4.1 – P2HFF#03)
	“Ao nível do ministério da saúde, havendo um conjunto de regras, é fácil ao ministério da saúde proceder a esta certificação. [...] Acabo por ver que em muitos aspetos ou a acreditação é imatura, e portanto muito filosófica, ou vai a um certo nível mas depois na prática não induz a diferença, não induz à alteração dos processos que deveria fazer.” (P5.V4.1 – P2HFF#03)
	“Os processos de certificação, acreditação, obrigam antes de mais as organizações a pensarem, a discutirem o problema, e depois a implementarem a melhor solução. Estes processos têm a vantagem de colocar todas as estruturas de uma organização, neste caso num hospital, a conversar, a definir processos comuns, procedimentos comuns, de acordo com legislação, normas, melhores práticas caso existem.” (P5.V4.1 – P4HFF#05)
	“Uma certificação seria uma forma de saber que foi implementada uma política de privacidade, mas também depois ir auditando. Isto porque as certificações não são eternas.” (P5.V4.1 – P1SPMS#02)
	“Se for só de infraestruturas eu diria que não é suficiente. Tem que ser mais transversal e focada nos dados, perceber se aquilo que fazemos com os dados está de acordo com as regras definidas.” (P5.V4.1 – P2SPMS#03)
	“A certificação pode ser um caminho a seguir. Tanto a certificação da proteção de dados como dos próprios sistemas. Os próprios sistemas muitas vezes não estão certificados. É um domínio que tem que se considerar no futuro.” (P5.V4.1 – P2SPMS#04)
	“A maior parte dos profissionais de IT não tem a formação adequada [em proteção de dados]. Esta certificação para a proteção de dados tem que certificar as práticas das pessoas. E para certificar as práticas das pessoas, têm que certificar as competências técnicas dessas pessoas.” (P5.V4.1 – P4SPMS#05)
	“As certificações acabam sempre por criar normas, regras, e conseguiríamos eventualmente garantir mais a privacidade da informação e transmitir segurança a todos nós, enquanto utentes.” (P5.V4.1 – P1HES#01)
	“A certificação é também um caminho para a proteção de dados. Para a certificação é necessário respeitar determinadas normas, determinados e protocolos.” (P5.V4.1 – P2HES#03)
	Este caminho [da certificação] é fundamental. [...] Já o conseguimos fazer ao nível a segurança, logo é possível caminharmos para uma certificação ao nível a proteção de dados.
	questões (por parte da SPMS, do ministério) em prol de uma certificação. Seria essencial.” (P5.V4.1 – P1HFF#01)
	“[...] aumentaria o nível de segurança e de confiança em relação à colaboração.” (P5.V4.1 – P2HFF#02)
	“É uma garantia, não é um seguro.” (P5.V4.1 – P4HFF#05)
	“Através de auditorias percebe-se se algo está mesmo a ser implementado, e se existe a necessidade de fazer alguma revisão, alguma melhoria. Poderia ser uma forma de atrair entidades externas para a questão da proteção de dados. Teria de ser sempre alguém do exterior a certificar.” (P5.V4.1 – P1SPMS#02)
	“Pode existir uma relação direta entre a questão da certificação e a confiança entre instituições. Alguém que seja externo e diga através de uma auditoria, que os processos estão bem implementados, que existem políticas implementadas devidamente, é uma segurança para quem está a ter um cenário de interoperabilidade ou outro. Confiamos um pouco mais por ter esse selo de certificação.” (P5.V4.1 – P1SPMS#02)
	“Caminhando-se neste sentido, e no contexto da partilha de dados através da PDS, uma certificação destas aumentaria a confiança entre as instituições. É necessário definir a que nível vai a certificação.” (P5.V4.1 – P2SPMS#03)
	“[...] sem dúvida um aumento na confiança entre instituições em matéria de partilha de dados.” (P5.V4.1 – P2SPMS#04)
	“Só que a proteção de dados depende de camadas, físicas obviamente, logicas [como é que são programados], e comportamentais. Poderia criar um ambiente mais seguro, mas tem que se certificar as pessoas. Fizeram ou não formação sobre privacidade e proteção dos dados? Estão ou não estão sensibilizados? Temos uma *workforce* que está preocupada com o assunto?” (P5.V4.1 – P4SPMS#05)
	“Certificando as instituições em matérias de proteção de dados, aumentaria a confiança na utilização da PDS.” (P5.V4.1 – P1HES#01)
	“Como benefícios, tínhamos uma certeza ou garantia que as politicas que são aplicadas numa organização são as mesmas, ou são no mínimo semelhantes às que estão a ser aplicadas noutras organizações.” (P5.V4.1 – P2HES#02)
	“Esta certificação aumentava a confiança entre as organizações que participam por exemplo em projetos como a PDS.” (P5.V4.1 – P2HES#02)
	“Aumentava a confiança entre organizações quando se partilha dados para uma organização certificada. Tenho a garantia de que estes dados vão ser usados de forma correta.” (P5.V4.1 – P2HES#03)

3. Data Display

P5	**Matriz de análise da opinião sobre P5. *Accountability* – responsabilidade e conformidade**		
Variáveis dependentes	*Padrão encontrado*	*Atitude proactiva da instituição* *(Que ferramentas podem influenciar a atitude e o compromisso da organização em relação à privacidade dos dados)*	*Influência sobre a privacidade* *(Que aspetos da privacidade dos dados são influenciados por uma atitude proactiva e são interoperáveis)*
P5.v1. Um programa de responsabilidade sólido e transparente, que contemple medidas adequadas e eficazes para pôr em prática as obrigações e princípios da legislação em vigor sobre proteção de dados, constitui a ferramenta operacional necessária para as questões da privacidade.	Utilidade/útil/confiança Diretrizes Proativa Nível executivo/tutela Equipa multidisciplinar Iniciativa conjunta	Não existe esta atitude de responsabilidade. Deveria haver uma atitude proativa em matérias de proteção de dados. Um programa destes poderia apresentar as principais diretrizes, que podem ser materializadas em medidas e políticas de privacidade. Este princípio da responsabilidade pode funcionar como um catalisador para estas matérias.	A privacidade é uma questão tão técnica como de gestão. Poderá haver um alinhamento dos grandes princípios de privacidade entre instituições. Pode ser uma iniciativa individual ou conjunta de todas as organizações para dar resultado. Promover mais a colaboração entre as instituições com base nas suas experiências - a elaboração de políticas de privacidade com base na experiência de múltiplos locais.
P5.v2. Um programa de conformidade constitui o meio de demonstração da vontade e da capacidade da organização em ser responsável e responsabilizada pelas práticas de gestão de dados. É essencial à salvaguarda da privacidade de dados, assim como à confiança do titular dos dados na organização, e entre esta e outras organizações. A eficácia e exigência das tarefas de conformidade dependem da sensibilidade dos dados, do volume dos dados processados e dos riscos específicos identificados.	Ferramenta [aplicável à privacidade dos dados] Análise contínua Auditoria/auditar Criticidade dos dados Exposição dos dados Risco Impacto Confiança Garantias	É possível, e desejável, fazer esta análise contínua de conformidade - perceber se as nossas ferramentas, processos estão de acordo com a legislação. Deveria ser uma prática comum para a proteção de dados - seria uma ferramenta fundamental. Auditar-se regularmente aquilo que é a utilização dos dados, à semelhança da segurança seria vantajoso. Dados mais sensíveis, mais críticos obrigam a uma maior preocupação. É importante a publicação deste tipo de análises e resultados em relação à proteção de dados.	À semelhança do que já se faz com os testes de robustez para as infraestruturas, deveria pensar-se em algo semelhante para os dados, para a sua proteção. O conhecimento de todos os processos de recolha e tratamento de dados é uma boa base de atuação. Se percebermos quais são os riscos em termos de informação, podemos depois verificar regularmente se estamos a conseguir eliminar o risco. Cenários de partilha de dados também deveriam ser auditados com mais frequência. A transparência da proteção de dados gera confiança no titular dos dados e entre organizações.
P5.v3. Os sistemas de *accountability* são essenciais à confidencialidade dos dados, ao disponibilizarem provas de evidência que permitem atribuir responsabilidade a comportamentos não esperados no domínio da privacidade dos dados.	Prova de evidência Prova de utilização	O *accountability* é quase sempre realizado de uma forma isolada. Estes sistemas são importantes para o contexto de partilha de dados, ao produzirem prova da utilização de dados. São uma garantia de que os dados estão a ser utilizados de forma correta.	Estes sistemas têm que de uma forma transversal acompanhar os dados, rastrear os dados, mesmo para lá do nosso sistema. Saber quem é que no outro sistema acedeu e alterou os dados. Se queremos ter partilha de dados, estes sistemas têm que funcionar integrados - tem que haver uma interoperabilidade técnica ao nível destes sistemas.
P5.v4. O desenvolvimento de rótulos de qualidade (esquema de certificação) para as medidas adotadas para uma gestão eficiente da conformidade legal, proteção e segurança dos dados, são no futuro uma ferramenta essencial ao desenvolvimento de um ambiente de interoperabilidade confiável e seguro em matérias de privacidade dos dados.	Garantia/mais-valia Confiança Complexo de implementar	Esta certificação seria uma mais-valia, uma garantia à existência de menos falhas na segurança dos dados. Tem que ser mais transversal e focada nos dados. Para garantir a certificação vou ter que garantir conformidade com todas as normas existentes. Devemos apontar para a certificação mas de uma forma discreta. A certificação deve ser vista mais como a garantia do funcionamento correto da proteção de dados. O custo e a complexidade dos sistemas podem condicionar o âmbito pretendido para este processo.	Estes processos têm a vantagem de colocar todas as estruturas de uma organização, a conversar, a definir processos comuns, procedimentos comuns. Ao nível do Ministério da Saúde, havendo um conjunto de regras, é fácil a este Ministério proceder a esta certificação. A certificação aumentaria a confiança entre as organizações, ao nível da partilha de informação. Tem que se circunscrever muito bem o âmbito para a certificação.